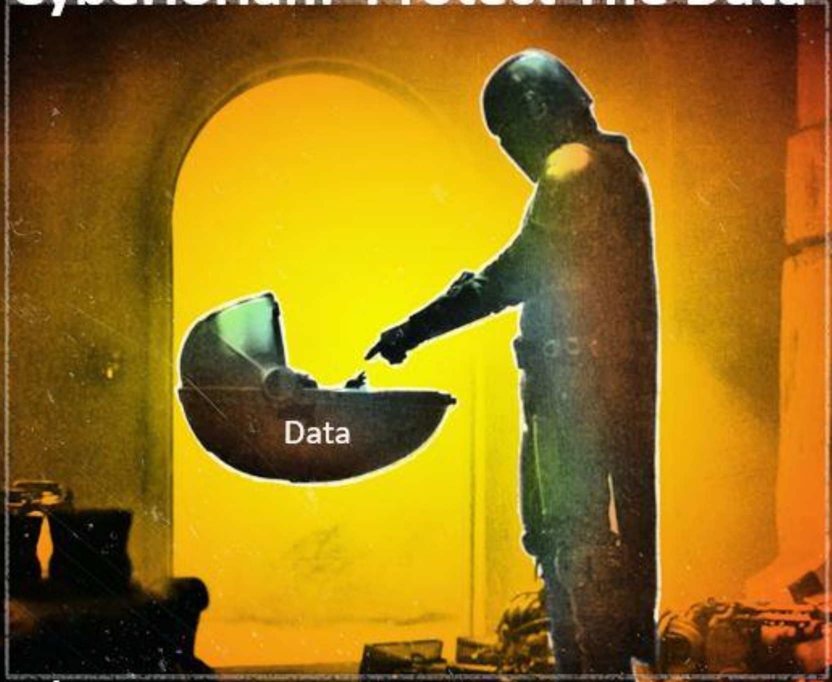
Cyberlorian: Protect The Data



9th Annual Hacking Conference

October 24-25, 2022

2

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Welcome To The 9th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Hidden Costs of Insecure Mergers and Acquisitions

Preparing for 'below the ground' costs

October 25, 2022

ISACA
Chicago Chapter

OPTIV

Contents

OPTIV

Speaking with you Today

Pradeep Sekar

Managing Director, Cyber Strategy & Transformation

Cybersecurity thought leader with extensive experience in delivering cyber strategy, M&A transformation programs for Fortune 100 and Fortune 500 clients.

Core expertise includes cyber strategy and risk governance, risk & threat profiling, benchmarking exercises, security assessments and transformation programs.

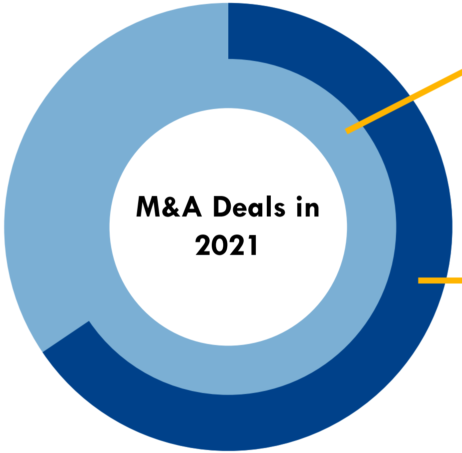
Service offering leader for Optiv's Security in Mergers, Acquisitions & Divestitures offering and leads the India Advisory practice at Optiv Inc.

OPTIV

M&A in Today's World

Modern day market features a wide range of dealmakers and deal kinds. The M&A landscape today includes significant participation from corporate purchasers, in contrast to the relatively straightforward deal market of 20 years ago, which was mostly composed of corporate buyers and some financial investor activity.

How Big is the M&A Industry?



$5.9T

Total M&A Deal Size in 2021

- Total M&A deal value reached all-time high with **62%** YoY growth rate

$3.8T

Total Corporate M&A Deals Size in 2021

- Witnessed a total deal value rise of **47%** YoY

Some industry-wise M&A deal values for 2021:

$1,100B **Technology**

$449B **Healthcare**

$60B **Payments**

M&A in other industry sectors including consumers, retail, energy etc. witnessed remarkable YoY growth.

Modern Trends in M&A

Source: Bain & Company, Baker McKenzie

OPTIV

Cyber Risks in M&A Transactions

Dealmakers are becoming increasingly concerned as a result of the nature and severity of the increasingly complex cyber security threats that have emerged over the past ten or so years during the M&A lifecycle.

Cyber Challenges in M&A Deals

Organizations lack the **ability to conduct due diligence** that can identify cyber-related strategic deal issues, hidden costs, and operational risks at an early stage of a transaction

Many M&A professionals are **unsure of the overall scope** of the risk they face from cyber attacks and data breaches. Most acquirers have very limited visibility beyond potential, point-in-time, subjective third-party risk scores

Organizations have **minimal involvement of cybersecurity teams,** and cyber is viewed as supporting rather than essential, especially in the early M&A lifecycle activities

Key Takeaways

32%

Businesses simply don't have enough skilled workers on hand with the abilities to recognize and draw attention to potential cyber security issues.

40%

Acquiring companies found a cyber security issue after the M&A deal was completed, a sign that the cyber due diligence is not performed properly.

63%

US chief executives said that they were extremely concerned about cyber threats.

83%

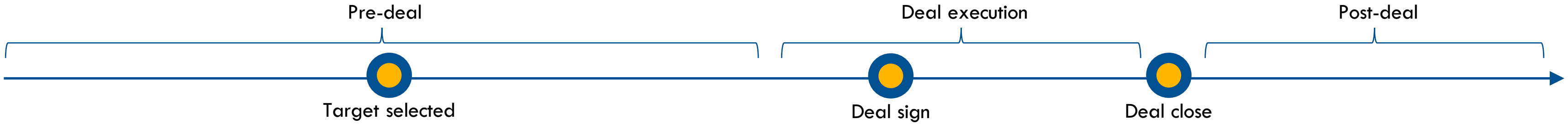
Customers will stop making purchases, following a breach, for several months, and one-fourth won't ever do so again.

Source: *IT Chronicles*

OPTIV

M&A Lifecycle

Transactions for MA&D typically go through the following four stages, in which each stage impacts the others. Security should be considered, if not heavily involved, across all four lifecycle stages.



1. TRANSACTION READINESS

Definition of M&A strategy to identify and prioritize potential targets

- **Define organizational M&A strategy**
- **Identify and prioritize M&A targets**
- **Develop initial valuations**

2. TRANSACTION DUE DILIGENCE

Screening and analysis of target's financial and operational health

- **Conduct due diligence**
- **Evaluate financial (balance, cash flow) and non-financial aspects (culture, integrity, operational synergy)**

3. TRANSACTION EXECUTION

Negotiation and execution of the transaction agreement

- **Negotiate transaction agreement with terms**
- **Execute the deal and closing procedures**
- **Plan for Day 1**

4. POST-CLOSE TRANSITION

Integration or separation planning and implementation activities

- **Perform integration/ separation planning**
- **Implement and execute integration/ separation plans**

Example security involvement

- Advise on key risks and potential security impacts
- Build customized M&A Playbook

- Perform due diligence research and analysis on target

- Support security-specific negotiation requirements
- Prepare for seamless Day 1 security support and transition

- Execute security transition plan
- Support seamless business and IT transition while reducing risk

Hidden Costs of Insecure M&A Transactions

Insecure M&A transactions attract a variety of hidden costs implying serious financial and reputational concerns with the potential to deem the M&A exercise detrimental and counterproductive!

OPTIV

Hidden Costs of Insecure M&A Transactions

Shrunk Valuation
Valuations drop as an inevitable result of the security incident at the target organization.

Fraud Penalty
Regulatory fines and penalty amounts subject to local laws for privacy breach / non-disclosures / lawsuit compensations etc.

Operational Disruption
Impact to business continuity prompting resource reapportionment for recovery solutions and high operational costs.

Above the Ground Costs

Inadequate TSA coverage
Costs arising due to lack of pre-defined cybersecurity-related services in the Transition Services Agreement (TSA).

Third Party Consents
Sprawl in third parties leveraged by the combined entity and managing security within contracts and agreements.

Below the Ground Costs

Maintenance of Redundant Systems
Maintenance of unnecessary / duplicate assets post integration due to lack of effective synergizing during the M&A transaction process.

Additional Cyber Insurance Coverage
Extended liability and costs on involved parties to cover for imprints of historical events or possible threats.

Insider Threat
Increase in risk posture due to enhanced likelihood of disgruntled employees (including contractors) impacting the M&A transaction.

Shadow IT
Costs due to security incidents arising from lack of adequate visibility into the unauthorized / unapproved assets.

Technology Debt
Additional investment to be made to mature the security program at target organization.

OPTIV

Shrunk Valuation

Security concerns at the target organization can prominently affect an M&A deal and negotiation process; one of the most implacable impact being sharp decline in valuation.

General Causes

- Historical breaches at the target organization
- Inadequate organization-level security infrastructure

Consequences

- Significant drop in valuation price
- Security concerns and complexities during integration processes
- Additional financial bearing for inadequate security measures

The Aftermath

Acquiring Company	Target Company
Plummeting valuation price affects overall portfolio value negatively, may also lead to a complete withdrawal of the deal	Decreases the ability to negotiate and close on a favorable price

Industry Speaks

$1.59M was the average total cost of lost business opportunities, representing the largest share of breach costs in 2021.

Case Scenario

Verizon Communications acquiring the operating business of Yahoo in July 2016 revealed two data breaches in 2013 and 2014 impacting over 1 billion user accounts. The initial sell-out price of about $4.8 billion was shot down by $350 million to a final price of $4.48 billion suffering approximately 7% drop with Yahoo! assuming 50% of any liability arising from the breach in future.

OPTIV

Fraud Penalty

Fraud penalties involve sanctions subject to breach of local regulations in terms of privacy, non-disclosures of historical security events, lawsuit compensations etc.

General Causes

- Unauthorized security protocols and controls
- Lack of security awareness in the organization
- Non-compliance to regulatory standards

Consequences

- Exorbitant penalties and legal fees for non-compliance
- Time and resources spent on legal proceedings
- Possible legal restrictions on daily business operations
- Reputational loss and cost of brand management

The Aftermath

Acquiring Company	Target Company
Unwarranted involvement in legal procedures for security-related events at target company	Obligations to provide penalty compensations to investor company and/or customers in case of deliberate concealment of security incidents

40% of acquiring businesses reported that they had discovered a cyber security problem after an acquisition, according to a report by West Monroe Partners.

Industry Speaks

Case Scenario

Marriott International acquired Starwood Hotels and Resorts Worldwide at $13 billion in 2016. Later, an internal investigation of a security notification revealed a data theft of up to 339 million customers including passport and credit card numbers in 2014. Marriott incurred over $28 million in recovery costs and faced class-action lawsuits and a fine of more than $23.8 million.

Operational Disruption

An insecure M&A brings larger risks in a combined entity owing to dependent and interconnected systems causing widespread disruption of business operations if not integrated securely and deeming the M&A process counterproductive.

General Causes

- Mounting technology debt pre-M&A
- Lack of periodic security reviews and internal audits

Consequences

- Halted business operations
- Sudden and massive loss of resources
- Huge recovery costs
- Third party withdrawals

The Aftermath

Acquiring Company	Target Company
Significant changes in resource allocation plans to accommodate recovery process hindering potential growth prospects	Disruptions in the operations of the target organization due to inadequate integration planning and execution

$188,400

is the average cost companies bear annually due to cybercrime; according to Insurance Information Institute.

Industry Speaks

Case Scenario

A global retailer organization had to shut down operations in one region for several hours, after an internal system malfunctioned. Further analysis of the incident revealed a misconfiguration that occurred while integrating with a local organization they had acquired recently, highlighting lack of proper integration planning and resilience testing post integration.

Maintenance of Redundant Systems

Due to the lack of effective synergies across systems during the M&A process, maintenance of superfluous or redundant assets can materialize unnecessary costs for the combined entity.

General Causes

- Systems maintained in silos in either organizations
- Unreviewed asset inventories
- Lack of cross-functional synergies within the organization

Consequences

- Un-inventoried assets going untracked and managed
- Unforeseen system breakdowns
- Operational inconsistencies
- Data duplications
- Lack of a single source of truth to rely during M&A processes

The Aftermath

Acquiring Company

Spiraling unwarranted year-on-year costs for maintaining redundant and/or legacy systems and process inefficiencies owing to duplicity

Target Company

Increased operational costs and unexpected downtime leading to difficulty in integrating with new platforms

Industry Speaks

53% of respondents discovered unaccounted IoT and OT devices after an acquisition. These factors have high chances of going undetected and invite abrupt changes in the systems architecture draining time and operations. (Forescout Technologies Inc., 2019)

Case Scenario

During an investigation involving acquisition of a transportation company by a regional retail company, it was found that about 6% of the IT budget was spent on maintaining end-of-life systems and duplicate assets which were unutilized. This led to operational inconsistencies and rising IT costs at the transportation company. The merged entity later underwent a series of rationalizing exercises.

OPTIV

Inadequate TSA Coverage

Costs resulting from the lack of pre-defined cybersecurity-related services post the M&A process in the Transitional Services Agreement signed between the two parties for smooth integration of business operations.

General Causes

- Inadequate review of agreement terms
- Lack of cybersecurity inputs while defining the TSA components
- Negligence of security requirements while drafting the TSA

Consequences

- Disruption of cybersecurity services
- Additional legal fees incurred at a later period for drafting additional requirements
- Chaotic integration processes
- Delayed decision making for critical operations

The Aftermath

Acquiring Company	Target Company
Unclear service agreements resulting in transfer of liability/ unfavorable terms for any security event arising post-merger unto the acquiring company	Obscure or lack of security-related services defined in the TSA leading to disruption in the cybersecurity capabilities at target organization

Case Scenario 1

Merger of two organizations in the hospitality sector surfaced security concerns for the internal systems of the combined entity within 2 months of operations. An internal investigation revealed that the concerned systems were not scoped as part of the cybersecurity services in the TSA.

Case Scenario 2

During the divestiture of Fortune 100 technology leader, absence of adequate cybersecurity requirements in the TSA agreement was identified post Day-0. Since the TSA was already in effect, amendments had to be drafted and signed, leading to a disruption in the services. Also, the seller had to incur overhead expenses for the management of the cybersecurity services till the amendments were signed.

OPTIV

Additional Cyber Insurance Coverage

Cyber insurance premium costs arise as a need to further quantify risks and determine real costs for concerned parties post M&A establishing liability in advance to compensate for effects of past events or potential security dangers.

General Causes

- Selection of a target organization with very low cyber maturity
- Lack of pre-M&A reviews of cyber insurance coverage and risk appetite for the combined entity
- Improper estimation of coverage required

Consequences

- Strain on organizational resources for recovery payouts
- Increased premium costs for acquiring additional coverage

The Aftermath

Acquiring Company	Target Company
Requirement of additional insurance coverage premium as per agreement between transacting parties	Liability of insurance coverage may be transferred to target company as per the transaction agreement

Industry Speaks

47% of the insurance clients are opting-in for cyber coverage in 2020, up from 26% in 2016; as per the 2021 report of the U.S Govt. Accountability Office.

Case Scenario

During the acquisition of a technology provider, lack of cybersecurity due diligence of the target organization led to the selection of a target with low-maturity cybersecurity program. This was identified by the acquiring organization's cyber insurance provider, resulting in a 21% increase in the subsequent insurance premiums for the acquirer.

Technology Debt

A delay in commissioning, decommissioning, or upgradation of existing assets and enhancing the security program maturity in line with the changing threat landscape can increase the technology debt, causing higher financial rollouts in the future.

General Causes

- Improper security assessments and timely gap analysis in technical requirements
- Lack of forward planning for IT and security functions
- Lack of IT and security thresholds
- Temptation to save costs in the short-term

Consequences

- Obstruction of critical functions
- Haphazard need to rip and replace affected technologies

The Aftermath

Acquiring Company	Target Company
Capital investments by acquiring company is redirected into reducing technology debt rather than avenues such as scaling of business and R&D	Unplanned recovery costs and diminished business performance, with negative impacts on the valuation price

Industry Speaks

57% of organizations that faced a cyberattack felt that patching their software would have prevented the attack. Moreover, **34%** said they were aware of the vulnerability before the attack, according to Ponemon Institute.

Case Scenario

During the acquisition of a large telecommunication firm by a Fortune 500 telecom giant, it was observed that the target company was running many legacy and outdated applications seeking to save money to extend the useful life of legacy systems instead of replacing them. This led to increase in technical debt to manage outdated / legacy systems.

Insider Threat

Risk exposure and theft of sensitive data is more likely during an M&A, especially from the buyer-side, as the convenience of moving sensitive data is higher during this process.

General Causes

- Employee dissatisfaction
- Motivated employee objectives
- Human error/negligence
- Slackened rigidity on compliance

Consequences

- Transfer of critical data to personal devices
- Loss of Intellectual Properties (IP)
- Exposure of trade secrets
- Exploitation of systems from external threats actors

The Aftermath

Acquiring Company	Target Company
Potential security breach and ensuing costs and liabilities	Detected compromise causing valuation/deal loss

Industry Speaks

51% of the organizations claimed that human error and configuration weaknesses were most likely to cause a breach during an M&A process, according to a Forescout study.

Case Scenario

During the acquisition of a US-based healthcare organization, the target company suffered data loss of thousands of patients, including name, phone number, and health history. The incident occurred due to deletion of data by an employee, owing to lack of training protocols, while migrating data from the target organization's on-prem environment to the cloud without ensuring backups.

OPTIV

Shadow IT

Costs associated with security incidents arising from inadequate visibility into the usage of unapproved or unauthorized assets in the organization.

General Causes

- Lack of rigid IT protocols
- Staffing inconsistencies and shortages
- Poor IT visibility on asset inventories
- Lack of due diligence assessments

Consequences

- High-risk governance failures
- Security and regulatory non-compliance
- Data theft and leaks
- Disaster recovery failures and loss of data

The Aftermath

Acquiring Company	Target Company
Additional time and resources to audit usage of unauthorized/unapproved assets in the merged entity and risks arising from such unidentified assets	Significant compensation costs to acquiring company for any such undetected practices before M&A

Industry Speaks

37% of IT professionals think that their organization lacks clarity regarding internal consequences for adopting technologies without IT approval with *77%* claiming unregulated shadow IT can worsen at their organization by 2025. (Entrust Datacard, 2021)

Case Scenario

After the acquisition of an insurance advisor by a financial services firm, it was identified that the target organization was using unapproved or unauthorized assets. These shadow IT applications were inherently less secure leading to vulnerabilities and potentially subsequent data breaches. Preventing and mitigating the shadow IT activities led to unplanned costs.

Third Party Consents

A M&A transaction brings with it a sprawl of third parties working with the combined entity and the need to manage secure contracts with each to avoid operational and compliance concerns.

General Causes

- Lack of security management within contracts and agreements
- Inefficient Third-Party Risk Management Program
- Lack of periodic third-party assessments

Consequences

- Increased probability of supply chain attacks leading to services failures
- Data exfiltration
- Non-compliance to security standards and regulatory requirements going undetected at the third-party organization

The Aftermath

Acquiring Company	Target Company
Delay in obtaining consent from existing third parties can lead to confidentiality issues and increased risk for the combined entity	Impact ability to define the attack surface of the target company along with increased reputational risks

Industry Speaks

$4.33M was the average cost arising from vulnerabilities in the third-party software which is one of the five most frequent first attack vectors, according to IBM's report on the Cost of a Data Breach (2021).

Case Scenario

Due to an ineffective TPRM program and improper access controls, a merger of two healthcare organizations raised security concerns. A lack of periodic third-party assessments caused a loss of $2.4 million during the merger, according to an internal investigation, and raised compliance problems with regulators.

OPTIV

Q&A

Secure greatness ™

How would you protect Grogu (Baby Yoda), if Grogu was sensitive data?

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Thank you for attending, remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

APPENDIX

Avoiding Hidden Costs of Insecure M&A Transaction

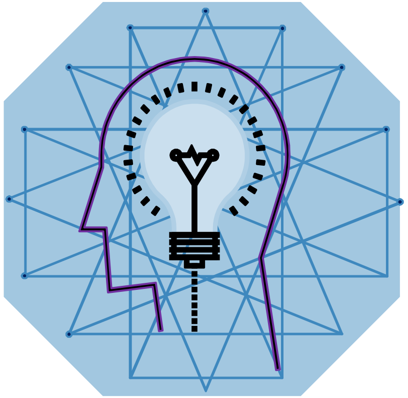
A continual effort is needed to create an executive-led cyber risk program, monitor progress, and continuously adjust the program to changing business goals and the evolution of cyber threats in order to attain and maintain a Secure, Vigilant, and Resilient posture.

CYBERSECURITY DUE DILIGENCE

- *Thorough verification and audit of target company's risk posture and historical assessments*
- *Evaluation of internal infrastructure such as network and data security, to identify pertinent gaps and facilitate an effective integration strategy*

SECURITY CONSIDERATIONS THROUGHOUT THE M&A LIFECYCLE

- *Define and implement security controls for effective identification and mitigation of potential risks throughout the M&A Lifecycle*
- *Leverage a Cyber Playbook for structured guidance on advancing cyber maturity while enabling business goals and driving investment value*



REGULATORY COMPLIANCE

- *Confirmation of adherence to compliance requirements of target company subject to industry and geography concerning data privacy and reporting*
- *Maintenance of an up-to-date repository to examine variations and duties going forward*

CONTINUOUS MONITORING

- *Evaluate the control effectiveness and monitor the cyber risk posture throughout the M&A transaction*
- *Conduct cyber post integration assessments, privacy reviews and compliance assessments*

OPTIV