Mastering the Art of Mergers and Acquisitions through Cybersecurity Due Diligence

By Reet Kaur
Reet Kaur

Work Experience
More than Twenty years of experience in Information Technology, Program Management, Corporate Finance, and Information Security. Built InfoSec programs at various Fortune 100 to 500 companies such as: Nike, Fidelity, CIBC and AECOM. Currently CISO at Portland Community College (PCC).

Education & Certs
Executive CISO: Carnegie Mellon University
Certifications: CISM, CISSP, CRISC, PMP Certified
Master Of Science (MS): University of Waterloo, Canada
Bachelors in Engineering: Punjab University, India

Interest & Hobbies
INTERESTS: Mentoring, Coaching, Education
HOBBIES: Always learning new things
FUN FACT: Worked as a Flight attendant as first job
Agenda

01. Intro to M&A
   Definitions and key goals.

02. Types and Process
   Different types of M&A and business process.

03. M&A + Cybersecurity
   Role of Cybersecurity for a successful M&A deal.

04. Due Diligence Challenges
   Common challenges in Cybersecurity Due Diligence.

05. Cybersecurity Risks
   Common cybersecurity risks involved in M&A transactions.

06. Best Practises
   Cybersecurity Due diligence steps for a successful M&A.
Merger
Union of two or more corporations by the transfer of property or assets of all, to one of them, which continues in existence, the others being swallowed up or merged therein.

Acquisition
The act of becoming the owner of a certain property or its assets.

Divestiture
Divestiture: to deprive; to take away or to withdraw.
<table>
<thead>
<tr>
<th>Objectives of M&amp;A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost Control</strong></td>
</tr>
<tr>
<td>Financial security for smaller companies as they merge with a larger firm which has the capacity and financial resources to handle the market storms.</td>
</tr>
<tr>
<td><strong>Eliminate Competition</strong></td>
</tr>
<tr>
<td>Decrease competition or create a monopoly status in the market. This eliminated competition and a solo status can prove very beneficial to the company.</td>
</tr>
<tr>
<td><strong>Synergy Effect</strong></td>
</tr>
<tr>
<td>Positive synergies improve revenue-generating ability, leading to product diversification, R&amp;D activities, market expansion and increased wealth for the shareholders.</td>
</tr>
<tr>
<td><strong>Market Power &amp; Share</strong></td>
</tr>
<tr>
<td>Gain a higher share in the market helps get the power of monopoly in the industry.</td>
</tr>
<tr>
<td><strong>Brand Image</strong></td>
</tr>
<tr>
<td>Post merger, the new brand enjoys the brand image of both the firms along with talent-sharing where the talents of reputed managers are put into this new firm.</td>
</tr>
<tr>
<td><strong>Diversification</strong></td>
</tr>
<tr>
<td>Ability to offer new products and services or entering into new markets or extending it to other regions or countries.</td>
</tr>
</tbody>
</table>
M&A – End to End Business Process

**Strategy Development**
Growth vision of the company.

**Target Identification**
Search and evaluate potential target companies.

**Valuation Analysis**
Operations, Customers, Financials, products to derive the true value.

**Negotiations**
Offer made, terms and process is negotiated.

**Deal Closure**
Final decisions to execute the transaction.

**Due Diligence**
Detailed examination to verify the target’s value and identify liabilities.

**Integration**
Both parties work together to ensure a seamless integration.

**Post Merger Compliance**
Both parties work together to ensure a seamless integration.

**Business as Usual**
Continuous monitoring of good standing and health checks.
M&A Information Security Strategy

Meet Business Goals
Enable the business with its M&A strategy through cybersecurity due diligence of the current security posture of the target company.

Identify InfoSec Risk
Identification of potential security, geopolitical or regulatory risks and signs of cyberattacks that could be currently happening in the Target company’s environment.

InfoSec Maturity
Reducing risks to the company during and post merger such as inadvertent loss of IP or exposure of critical assets or any sensitive information.

Contain Cost
Identify and Quantify valuation considerations including estimated one-time and recurring costs to remediate cyber security control gaps while protecting deal value and strategic drivers.
For many organizations, barriers that make this challenge difficult to address include:

**Inclusion**
Security leaders are often kept out of the loop during the early stages of an M&A.

**Processes**
For most organizations, M&As are rare occurrences, which means that security teams do not have pre-developed playbooks for due diligence.

**Time**
The result is that a large majority of security leaders are not given enough time to conduct due diligence, and then they have to spend some of that precious time just developing their due diligence playbook.

**Skills Shortage**
There is a lack of due diligence skills and experience on security teams with M&A transactions.
InfoSec Due Diligence Challenges in M&A

Not Enough Time

64% of companies believe that they are not given enough time to fully assess a target’s security risks prior to acquisition.

Lack of Skills

63% of companies believe that they do not have the right skills to adequately conduct cybersecurity due diligence on an acquisition target.

Source: ForeScout, 2019
Cybersecurity Risks in M&A

Insider Threats
Negligence and deliberate sabotage. Unreported data breaches – stop or delay the deal

Customers
Acquiring targets with poor cybersecurity and privacy hygiene will cause customer mistrust

Existing Hygiene
Dormant hackers within the target’s network can find a new opportunity to strike after M&A. Existing vulnerabilities and poor cyber hygiene of targets will be inherited and will have to be remediated

Regulations
Increased Scrutiny on M&A deals by Regulators. Regulators raising fines for non-compliance

InfoSec Risks to M&A
Case Study - M&A Gone Wrong

13 Billion Dollar Deal

YEAR: 2015
Data Breach - Lessons Learnt

2015-2018 - Starwood hackers remained undetected

Security team either left or were laid off shortly after the acquisition.

Hackers had stolen data on as many as 500 million guests.

Multiple Lawsuits but Marriott's Cybersecurity Insurance covered most breach costs

Perform thorough due diligence of security controls and compromise assessments during the due diligence phase.

Retain talented security staff when acquiring a new company.

Continuously monitor for potential attacks or malicious activity during and after a merger is complete.

Cybersecurity insurance is critically important during M&As, but not fully reliable.
Cyber Security Due Diligence Steps
01. Prepared InfoSec Insurance

- Preparing your cybersecurity insurance for a potential merger or acquisition
- Evaluate current state of cybersecurity insurance
  - Ensure policy will cover any new acquisitions
  - M&A related security risks
- Assess both cybersecurity Insurance policies to identify additional needs
## 02. Third Party Assessor

- Target companies usually unwilling to share too much information with buyers
- Consider retaining a third-party assessor to assist with due diligence activities
- Inadequate in-house security expertise for rapid due diligence
- Third party with expertise and ready-to-go tools can save significant time during due diligence phase
03. Discovery / Workflows

- Gather the documentation and list of:
  - Information security staff and vendors including Information security providers (MSSP’s or MDR’s)
  - Security controls, tools and In-flight or planned information security projects
  - Track and collect all documentation required for cybersecurity due diligence
    - Documentation and information flows determined by the target organization
- Manage Workflows & Conduct Discovery / Interviews
04. Compromise Assessment

- Assess capability to detect and respond to compromises
- Assess the effectiveness of detection capabilities by reviewing detection controls
- Identify if each detection control is working or not or if any evidence of compromise has been detected
- Evaluate if additional detection tools will be required with associated costs and timelines
- Deploy temporary detection tools into the target organization to build confidence that they are not already compromised
- Indicate the confidence of diagnostics
05. Risk Management

- Perform Risk Assessments
- Frame identified risks and evaluate the threat type, risk impact and likelihood of the risk to occur within 1st year of M&A to derive the risk rating
- Assess if the risk is beyond your organizational risk tolerance limits
- Recommend risk treatments for each identified risk
- If risks are above tolerance and cannot be mitigated or transferred, they can be rejected
- Describe and document proposed mitigation plans along with associated costs and times
## Cybersecurity Due Diligence

| 01 | Insurance |
| 02 | Third Party Assessor |
| 03 | Discovery/Workflows |
| 04 | Compromise assessment |
| 05 | Risk Management |

### 06. Communicate

- Present cyber risk assessment to M&A team
- Focus on risks that exceed risk tolerance
- Share results of Compromise Diagnostics
- Risk treatment costs (mitigation and transfer) may alter the nature of the deal
- Be a problem solver - Your job is to help KNOW the risks and not to say NO
- Present mitigation plans and associated costs to help negotiate the deal purchase price
Cybersecurity Playbook - Keep it Handy

01 Screening

02 Due Diligence
Assess InfoSec risk & capabilities. Conduct cybersecurity risk and/or compromise assessments. Evaluate security and compliance posture. Evaluate the potential cost of cybersecurity to factor into deal value.

03 Strategic Plan
Business enablement strategies. Ensure collaboration and improved productivity. Pick best from both sides to elevate cybersecurity program.

04 Tactical Initiative

05 Closure
Integrate and improve cybersecurity. Continue to monitor.
ANY QUESTIONS?
IF NO, THEN JUST CLAP!
M&A cybersecurity framework

IMO

Cybersecurity PMO

**Governance**
- Enable business goals
- Reduce cyber risks
- Advance program maturity
- Contain BAU cost

**Strategy**
- Network & infrastructure
- IAM
- Application security
- Security operations
- Endpoint protection

**Capability**
- Data protection
- Insider threat
- Third party risk mgmt.
- Training & awareness
- Security compliance

**Deal cycle**
- Day 0: Due diligence, Risk prioritization
- Day 1: Integration strategy, Deep-dive capability analysis, Risk remediation
- Day 100: Continuous risk monitoring
- Day 100+: Tech & process integration, Target operating model, Business solution enablement

**Execution**
- Risk remediation
- Capability integration
- Cost rationalization
- Change management
- Continuous monitoring