MANAGING INFORMATION SECURITY CHALLENGES DURING MERGER AND ACQUISITIONS

DR. AISHA.M.SHERIFF*; ANJAN BABU K**

*Professor,
Bahadur Institute of Management Sciences,
University of Mysore, Mysore, India.

**Research Scholar,
Bahadur Institute of Management Sciences,
University of Mysore, Mysore, India.

ABSTRACT

Merger and Acquisitions are widely preferred growth drivers in Competitive Markets & Economies & Organizations perceive Merger and Acquisitions as explicit means to increase their stronghold in domestic or foreign markets. Merging entities have disparities in information security policies. Information Technology (IT) infrastructure, Network Audit & Compliance issues are imperative in current scenario.

IT & its facets were never really considered important or was not given due importance during Due Diligence in Merger & Acquisitions process. Companies realized the loss only when data loss or leakage became pre-dominant for the failure of Merger and Acquisition. The Organizations should take this Area of study strategically to avoid pitfalls due to pilferage.

This paper focuses on the approach adapted by the organization in achieving Information Technology integration in Merger and Acquisitions process. But Mergers and Acquisitions face challenges in the form of cultural, technical and regulatory issues.

KEYWORDS: Information Security, Merger and Acquisitions, SOX.

INTRODUCTION

In good times and bad, it seems as though mergers and acquisitions are supposed to create new, stronger organizations. There are many good reasons for growing the business through an acquisition or merger. These include:

- BETTER INDUSTRY KNOW-HOW : Access to good management and know-how enhances better prospects for acquirer
CUSTOMER BASE AND INCREASING YOUR MARKET SHARE: Target business may have distribution channels for better market connectivity.

DIVERSIFICATION OF THE PRODUCTS, SERVICES AND LONG-TERM PROSPECTS OF YOUR BUSINESS: A target business may be able to offer you products or services which you can sell through your own distribution channels.

REDUCING COSTS AND OVERHEADS: increased purchasing power and lower costs.

REDUCING COMPETITION: Purchasing new intellectual property, products or services increase revenues through Research and Development.

ORGANIC GROWTH: Businesses in the same sector can combine resources to trim down costs, eliminate duplicated facilities or departments and increase revenue.

Acquiring a small player in foreign market leverages access to greater market share. Smaller companies achieve higher returns on their brand management activities.

For an organization, decision to merge is an easy part. The real challenges come into foray after the acquisition of the new entity and the needed changes in people management process technology systems and compliance. The current paper focuses on information technology challenges in mergers and acquisitions.

Any cross border merger and acquisition involves uphill tasks as the merged organization would have disparate systems, different IT infrastructure, different hardware, different protocols, and different technical architecture. Hence, the challenge lies in the integrating and consolidating IT. However, this paper focuses on the approach adapted by the organization in achieving IT integration in merger and acquisition process.

CHALLENGES IN M&A

The challenges can be generally categorized into Cultural, Technical and Compliance.

(A) CULTURAL CHALLENGES IN M&A

In a recent survey by McKinsey and the Conference Board, 50 percent said that “cultural fit” lies at the heart of a value enhancing merger, and 25 percent called its absence the key reason a merger had failed. But 80 percent also admitted that culture is hard to define. The cultural due diligence on various dimensions like environmental values, innovation, motivation co-ordination control accountability should happen during the deal process giving executives more time to design the merger in a way that builds cultural assets and mitigates risk. Cultural due diligence signals management approach of companies to world through its corporate websites, annual reports, speeches, news articles, blogs, stock market filings, recruiting, and mission statements etc. The analysis of the publicly available information should be surveyed and could be kept confidential before the merger deal.
(B) TECHNICAL CHALLENGES IN M&A

Mergers bring about the revamp of technology infrastructure and processes. Employees prefer to get back to normal. This could be easier if employees can continue using the technological tools of one or more of the merged firms or if at least one of the firms used virtual environments before the merger. In this case document management systems help the newly created entity to access the shared information of acquirer and acquiree. In this context corporate managers should be aware of treating risks in IT as high priority. The common regime of transfer of technologies and processes should be established to operate.

(C) REGULATORY CHALLENGES IN M & A

An organization's compliance mandates are often driven by the industry in which it operates. Financial companies are required to meet the provisions of the Sarbanes-Oxley Act (SOX) and Gramm-Leach-Bliley Act (GLBA). Health Insurance Portability and Accountability Act (HIPAA) for healthcare verticals, and banking service verticals have to meet the Payment Card Industry (PCI) Data Security Standard.

The commonly applicable regulations are the most critical issues to consider are access management, information security policies, protection of customer data and monitoring and testing. M & A should comply with the new regulations that may require additional understanding and implementation.

MAKING MERGERS WORK

When merged or acquired the organization need to:

- Inform end users of both about the impact and necessity of merger.
- Implement change management process and communicate to employees.
- Integrate systems and implement new policies and procedures that leverage best practices

(I) SAFEGUARDING INFORMATION SECURITY

Merging entities have discrepancy in information security policies. These policies have to be reviewed, combined, aligned, later perform a gap analysis, assessing both organizations against the new policy. Generate a roadmap that states which procedural and technological changes will be needed for both companies to comply.

Information security consolidation is the best approach and involves:

- Aligning information security policies
- Implementing a strict information security regime
- Investing in information security sensors
• Creating roadmap technological changes.

The consolidation of policies, technical areas must be addressed at once, to shore up an organization and prepare it for attacks because as soon as the merger process begins, an organization could be vulnerable.

WIRELESS LAN DEPLOYMENT

If one entity relies heavily on Wi-Fi but the other does not, there may be a considerable distinction in their vulnerability profiles. Rather than ripping wireless out of the organization, check the security settings of their wireless infrastructure. If it lacks encryption or has weak authentication, boosting it with improved technology, such as WPA2.

USBs

To lower internal data security breaches and other insider threats, companies may choose to disable USB devices on laptops. Before choosing this route though, it’s important to consider the political and functional ramifications of such a move.

MALWARE AND IDS TOOLS

Invest in healthy anti-malware and anti-spyware that regularly reinvents itself and provides regular and critical patches..

FIREWALLS AND IDS TOOLS

After the merger is complete, the security team should monitor for large amounts of data being transferred outbound across the Internet. Depending on employees’ "normal" Internet usage patterns, companies may want to set up a scan for any FTP or HTTP transfer of a file greater than a certain scale. Any violation could be a sign of data exfiltration. Monitor Web proxy logs as well to determine if attack tools are being downloaded and used inside either company.

Successful execution of the above strategy can help merging entities significantly lower their exposure.

(II) CONSOLIDATION OF NETWORK ARCHITECTURE

Organizations should spend substantial time documenting the network architecture showing Internet and business partner connections for the merged organizations. Ensure both companies are capable of monitoring their DMZs and vital internal networks, specifically with intrusion detection system (IDS) sensors. During merger deploy supplementary sensors in both companies. Tune them to look for the most likely attacks, focusing on Windows issues, Web application attacks or other types of threats common to a given environment. Assign information security personnel and system administrators from both companies to analyze the IDS alerts to determine if systems have been compromised.
(III) DISASTER RECOVERY MANAGEMENT

In the merger process, an organization’s proprietary data & IT infrastructure are among the most valuable assets. It is important to ensure that these assets are restored. The potential loss of important assets such as data, hardware, and software is too great a risk to ignore. With the added cost of downtime and loss of assets, the results can be staggering.

(IV) NETWORK AUDIT

Network infrastructure plays an vital role hence network audit is to be conducted to categorize loopholes or recommended improvements in your IT infrastructure.

(V) COMPLIANCE ISSUES IN M & A

From a merger perspective, SOX auditors and regulators will look for reports on access management controls. Before the auditors arrive though, there are some key questions security pros should ask to ensure both companies are on a level playing field:

- What types of access management systems do the two companies use?
- Are they both on Active Directory, or is one using LDAP while the other uses something else?
- What's the current state of audits of accounts at both companies?

GLBA has similar provisions to SOX, but it's more focused on protecting customer data rather than access management. GLBA calls for:

- Encryption of confidential data
- Use of strong passwords for accessing systems, limiting employee access to customer data, and physical security for customer records.

As with SOX, in an M&A situation, the security teams should compare each organization's:

- Encryption methods
- Customer data-handling procedures and overall adherence to their respective information security policies.
- Policies and procedures, which will need to be adjusted to common standards for both organizations.

In an effort to make the entire process easier, merged entities must create compliance, for the melded entity. People from both entities should work out a plan to achieve compliance harmony.
CONCLUSION

Mergers and acquisitions are common headlines in today's information security world, and that's great news for malicious hackers and data thieves. When companies join forces, they often leave themselves open to attack. Hence integrating Information technology and consolidation becomes strong business driver for the success of Merger and acquisition. In order to get the expected benefits from the merger, however, the new organization would have to rationalize its technical architecture, standardizing systems and applications platforms. Hence a strategic approach should be adopted by organizations to meet the objectives of the M&A.

REFERENCES