Infosys®
Navigate your next

VIEWPOINT

HOW IMPORTANT IS DATA PRIVACY IN MERGERS AND ACQUISITIONS?

M&A transactions will always live or die based on financial and market analysis. However, data privacy and security must not be an afterthought, but instead be built into the data, technology, and governance mechanisms undergirding the deal itself. The result? Increased customer confidence, improved regulatory approval rates, and a healthy balance sheet.

Infosys® | Knowledge Institute

Despite a global recession that froze deals for months, the value of mergers and acquisitions (M&A) in 2020 was down only 5% from the previous year. Salesforce bought Slack for $27.7 billion[1], and the overall merger value in the U.K. exceeded $200 billion in the fourth quarter, according to data provider Dealogic.[2] Overall, businesses worldwide still spent $3.6 trillion last year in M&A transactions.[3]

Bigger firms acquired smaller ones to get the right dose of technology, scale, portfolio diversity, and financial efficiency. Data was traded; customers were brought onboard; and deals closed with a hurrah of stock market activity. But amid all this movement, regulators had to determine whether the merged entities were compliant with European Union and U.S. regulations and whether customer data was secure.

There are good reasons for all this due diligence. A major data breach or compromise can damage the global financial market, hurt smaller vendors in corporate ecosystems, and tarnish M&A transactions. In 2017, Verizon lowered its offer to buy Yahoo by $350 million after learning that 3 billion Yahoo accounts had been hacked.[4]

> A major data breach can tarnish M&A transactions and damage the global financial market

M&A transactions are a favorite topic for analysts. They ultimately determine the value of the merger based on financial data and market movements. Even so, data privacy and security must not be an afterthought, but built into the technology and governance mechanisms undergirding the deal itself. A security failure could cause a transaction to crumble at the last minute. Companies must delve into their partners' data breach histories to understand whether things could get worse once the merger goes through. Meanwhile, a road map should be in place so that the new corporation is fully compliant with regulations at home and abroad. All these issues are fraught with complications and keep chief financial officers up at night.

A holistic data privacy approach

What if the M&A deal itself had all such privacy concerns built into its topology? In this paradigm, companies are screened and valued with full legal oversight that marries privacy and security exposure with the systems in place once the deal goes through. In this case, people, processes, and technology not only comply with privacy regulations but also help derive further capabilities for the merged corporation. To build this paradigm, any M&A deal must include the following four critical stages.

1. **Companies need to thoroughly understand privacy exposure during the screening process.** If a business is noncompliant, the risk of privacy exposure must be built into the deal's value. Any discount resulting from that risk will depend on the potential revenue earned from customer data post merger. Data analysis can help determine those calculations. Also, the acquiring firm would have to spend an undetermined amount to bring the merged entity into compliance with existing regulations. To help in this sort of screening, a compliance maturity measure can compare the M&A cost target with the cost of acquisition. If compliance maturity is low, the acquiring company might want to forgo the deal.

2. **Data privacy due diligence should be conducted with a data room in place.** Along with the basic risk audit, companies should carry out a vulnerability mapping exercise (think penetration tests and vulnerability assessments). These put both companies in the same "data room" to discuss what internal data is collected at each firm, why it is collected, and how the combined data footprint will look post merger. It also means working out what to do with personally identifiable information (PII) and creating a confidentiality agreement that covers unknown reputational risk. A data room ensures that regulators are happy with the deal post merger and potentially heads off fines. The data room also ensures that pre-merger firms do not disclose sensitive customer and competitive information. Care must be taken to set up the data room so that:

- It is "clean," i.e., tightly controlled, with consent required before the sharing of customer data.
- No data downloads or extractions take place.
- Data is aggregated to avoid sharing information about real people.

3. **The deal structure needs to include data privacy.** Companies should map out what data is held, how it is processed, and what regulations, if any, the processing of this data must meet. In any agreement, if consent and data transfer agreements aren't compliant with global regulations, the sale of data between the firms will be null and void post merger. Further, both firms have to ensure that customers are aware of the transaction and how data will be used in the merged entity. The deal structure between the merging firms also needs to ensure that disputes can be handled efficiently and robustly, which requires a warranty agreement. This agreement factors in any investigations or complaints.

4. **Both firms need to integrate interrelated IT systems and migrate data after the deal is finalized**. This stage ensures business continuity and updates employees and partners on data privacy policies. As part of this exercise, the following things should happen:

- Detailed discovery should be performed to identify personal data footprints in the merged entities, with a joint data inventory mapped

out. The process of discovery can be fast-tracked by using artificial intelligence to scan unstructured data (often an uphill task).

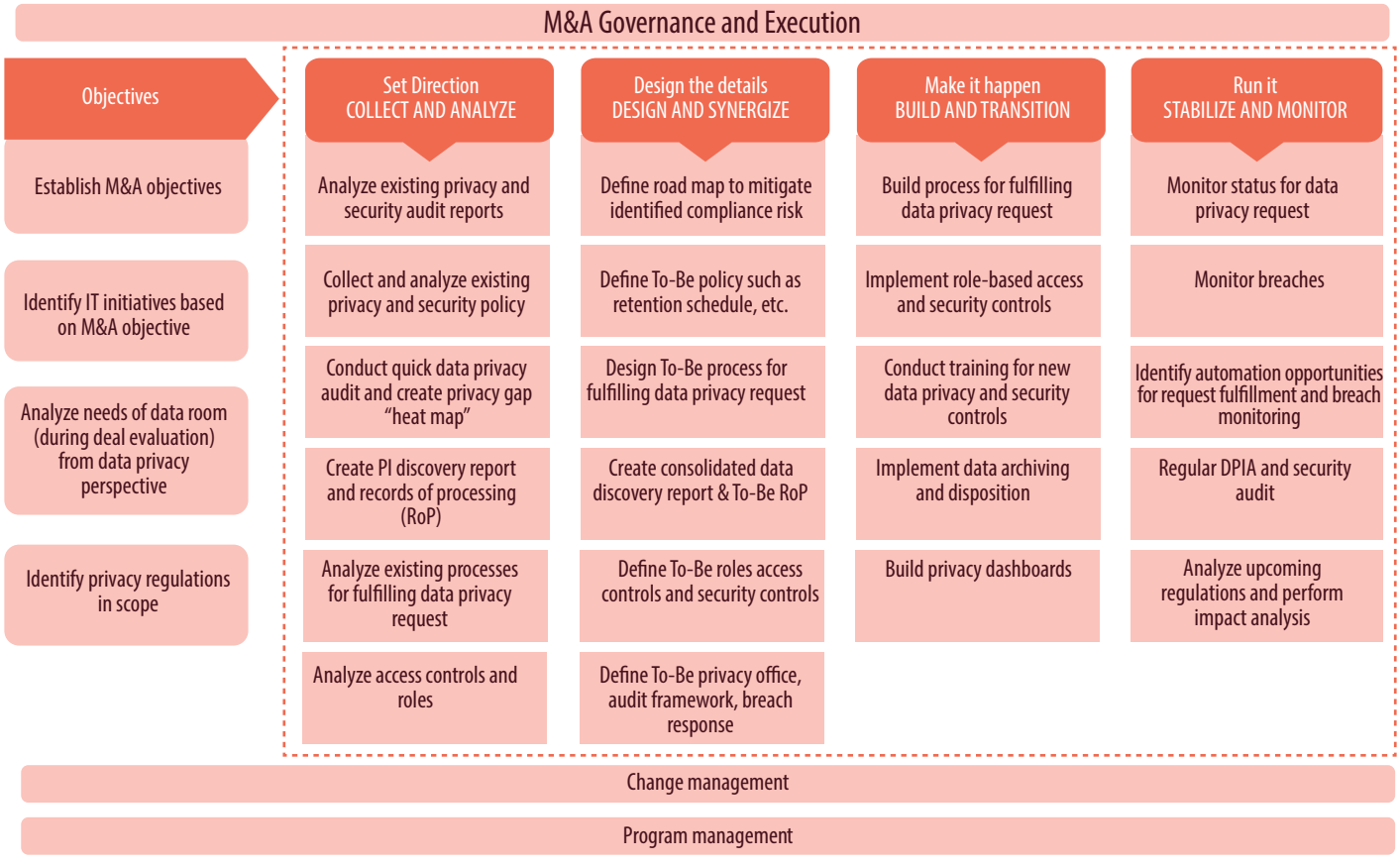
- Records of processing are devised to ensure that data is used in the way it was originally intended.
- Customer consent is established, with the thorny issue of how contradictory customer files — common to both merged entities — are processed.
- Data privacy policies and guidelines for the merged entity are designed and implemented.
- A change management training plan is created to ensure employees understand and embrace changes in privacy policies and processes. Current privacy regulations clearly outline the need to train employees and are the responsibility of the acquiring organization.
- Access rights from both organizations are defined in data subject access requests.
- The target operating model of the merged firm is defined, whether it is decentralized, centralized, or hybrid.
- Along with creating an effective post-merger business and operating model, the success of an M&A deal often resides in how quickly and seamlessly the integration phase is completed and how soon synergies are unlocked. Data exchange, quality, and governance technology increase the speed of implementation by automating much of the process and also reduce the chance that human intervention leads to a data breach.

The data privacy framework

Managing data security in a comprehensive way is a major undertaking. Companies need to take care of many moving parts, bring together diverse teams with different skill sets, and keep up to date with the pace of innovation in technology and operating models. At Infosys, we have found that established frameworks and reference architecture for data privacy add another level of insurance to M&A deals. The framework below (Figure 1) includes program and change management, and also governance and execution processes across four stages: collect and analyze; design and synergize; build and transition; and stabilize and monitor.

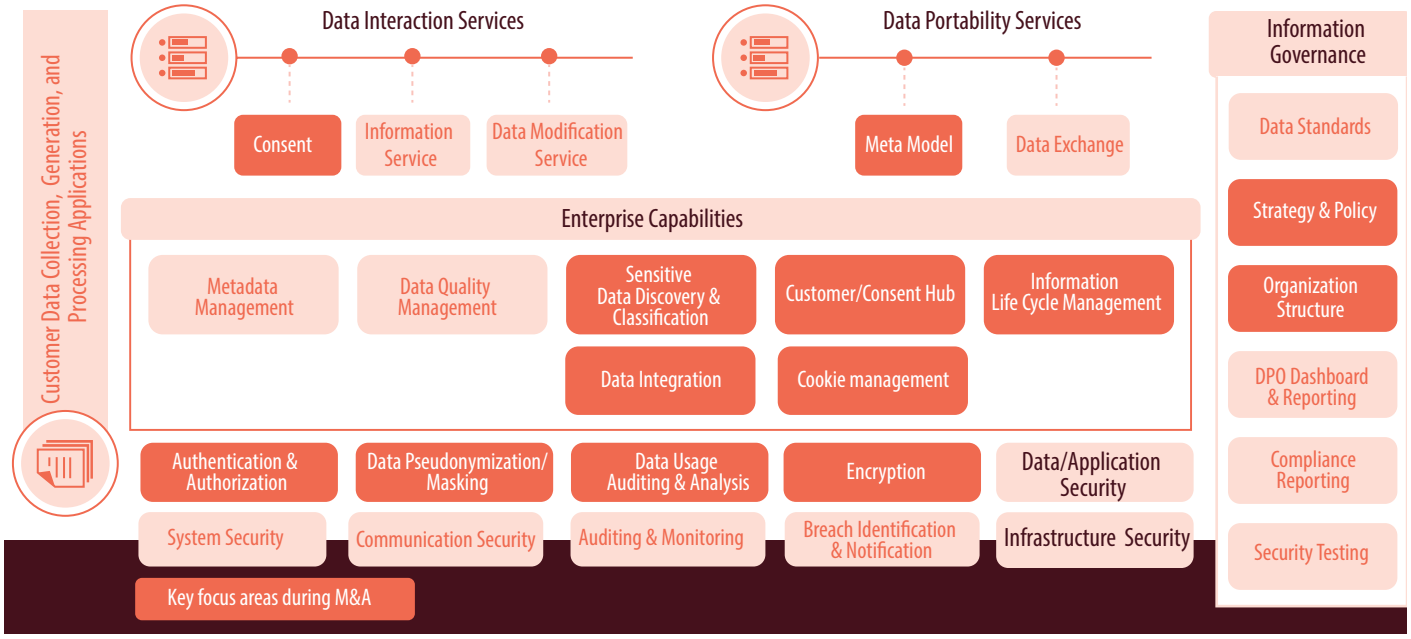
- **Collect and analyze —** The as-is status is analyzed and processes are documented. Workshops help identify gaps and risk with respect to data privacy, ethics, and regulations — before a gap assessment is conducted.
- **Design and synergize —** The overall privacy architecture and operating model is defined and designed. Based on the gap reports and workshops, a road map is laid out for the acquiring organization.
- **Build and transition —** This is where implementation of the target operating model happens. Various mechanisms and measures are built

Figure 1. Infosys data privacy M&A framework



Source: Infosys

Figure 2. Reference architecture to ensure regulatory compliance



Source: Infosys

to test capabilities. Also, policies and procedures are implemented or revamped in response to the gap analysis report.

- **Stabilize and monitor —** A trusted partner can supervise and assess the ongoing risks and output.

Working with large global clients, Infosys has developed a comprehensive reference architecture detailing various data privacy issues. Some nuts and bolts are more important to M&A transactions than others (Figure 2).

- **Data interaction services —** Needed to interact with data subjects, including the customer, supplier, vendor, or employee. Their key function is to present privacy policies and to capture privacy rights requests and consent from data subjects.
- **Data portability services —** Enable secure data exchange between organizations and subjects, fulfilling data privacy requests.
- **Enterprise capabilities —** These are data management capabilities that fulfill privacy rights and ensure data is processed in line with organizational policies.
- **Data/application security —** These capabilities allow the organization to store and process data securely, while preventing breaches and access of data by unauthorized individuals.
- **Information governance —** Defines the structure of privacy throughout the merged organization and includes the privacy policy, data policy, and privacy-reporting-related components.

Moving ahead

Instead of being led from the top down and in silos, we believe different teams — from finance to operations to technology — should work with the same data from day one. Such a composite privacy merger management unit would also use data analytics and artificial intelligence to unite financial, operational, and commercial due diligence.

Data privacy and security can make or break a deal or significantly change the transaction cost. It is important then, before the hard legwork, that CXOs ask themselves: "What do we stand to win from this deal?" and "How will the merged operating environment enable these business outcomes?"

> A privacy merger management unit would use AI and data analytics to unite financial, operational, and commercial due-diligence

When adding privacy and security risk to the equation, executives sometimes determine that the cost of acquisition is too great to justify the projected return on investment. Or they might decide that significant restructuring is needed to ensure that the deal will provide competitive advantage.

If the business value of merging is just too good to pass up, as dictated by the combined estate of people, processes, and technology, then a road map and reference architecture must be put in place to mitigate data privacy and security risk. This will ensure the deal goes through smoothly, is approved by regulators, and delivers long-term business value as determined by improved customer confidence, reduced threat, and a healthy balance sheet.

References

1. M&A rebounds sharply to hit $3.6tn in 2020, Ortenca Aliaj & James Fontanella-Khan & Arash Massoudi, Dec 31, 2020, FT
2. U.K. Gets In on Global M&A Surge, Ben Dummett, Jan 18, 2021, WSJ
3. See Ref 1
4. Due Diligence on Cybersecurity Becomes Bigger Factor in M&A, Kim S. Nash & Ezequiel Minaya, March 5, 2018, WSJ

Authors

Gaurav Bhandari

AVP – Infosys
gaurav_bhandari@infosys.com

Varun Khanna

Senior Consultant – Infosys
varun.khanna02@infosys.com

Harry Keir Hughes

Senior Consultant – Infosys Knowledge Institute
harrykeir.hughes@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next