AN FTI CONSULTING WHITE PAPER
SEPTEMBER 2019

PROTECTING DEAL VALUE: A CYBERSECURITY POINT OF VIEW

Managing Cybersecurity-Related Merger and Acquisition Risks

Once typically excluded from the mergers and acquisitions ("M&A") due diligence checklist, cybersecurity as a list item has gained importance as incidents of data breaches in recent years have rippled through the business world, exposing vulnerabilities in information technology ("IT") infrastructure and systems and resulting in many millions of dollars in damages.

A successful post-acquisition process entails integrating the IT infrastructure and applications of the two organizations. The data elements to be protected by each organization include sensitive employee/customer information, sources and storage of data, and intellectual property. Despite the paramount importance of these elements, cybersecurity is often minimized on an already lengthy due-diligence list. Cybersecurity is not often evaluated and prioritized by management with the same rigor as other deal components such as financial, tax, and legal items during both the pre-acquisition due diligence and integration processes. This introduces risks that, if not identified and mitigated early, might have a high impact on value realization.

VERIZON'S DISCOVERY OF A PRIOR DATA BREACH AT YAHOO! RESULTED IN A $350M ADJUSTMENT TO THE PURCHASE PRICE (7% OF DEAL SIZE).

To help management understand whether either company involved in the transaction falls into a high-risk category from a cybersecurity perspective, listed below are five key questions to ask regarding the transaction:

1. Is it a cross-border transaction that warrants data compliance considerations such as GDPR?
2. Is a company with a traditional IT environment acquiring one with a SaaS-, PaaS- or IaaS-based environment?
3. Is a company with conventional data warehouse/business intelligence capabilities acquiring a company with a focus on Big Data?
4. Is Internet of Things ("IoT") capability a fundamental consideration in IT and operations?
5. Have the companies involved had any notable security incidents in the past that were publicized or subject to litigation?

THE MERGER PROCESS BETWEEN TWO HOSPITALITY COMPANIES, WHICH KICKED OFF IN 2016, UNCOVERED A DATA BREACH THAT STARTED IN 2014 AND WAS ONGOING WHEN THE LOYALTY PROGRAMS AND MEMBERSHIP DATASETS WERE BEING MERGED. IT WAS ESTIMATED THAT THE PERPETRATORS MAY HAVE STOLEN RECORDS FOR AS MANY AS 383 MILLION CUSTOMERS.

This paper will focus on M&A-driven IT integration and offer an approach to tackle some of the most pressing issues in the cybersecurity arena.

UNDERSTANDING CYBERSECURITY RISKS

Historically, M&A due diligence focused on "traditional" risk areas such as financial, operational, and IT infrastructure capabilities and transition. However, with notable data mega-breaches such as Telstra and Yahoo!, it's clear that cybersecurity should be considered a top priority for executives. Gone are the days when security was an afterthought in the M&A process.

MERGERS AND ACQUISITIONS OFTEN RESULT IN AN INCREASED ATTACK SURFACE FOR THE COMPANIES INVOLVED. WHEN COMPANIES INTEGRATE THEIR IT ASSETS, A THIRD PARTY THAT SUCCESSFULLY COMPROMISED ONE OF THE COMPANIES COULD USE THAT ACCESS TO COMPROMISE THE OTHER(S). FOR INSTANCE, IN 2015 THE AUSTRALIAN TELECOM FIRM TELSTRA ANNOUNCED THAT THE NETWORKS OF ITS RECENTLYACQUIRED SUBSIDIARY PACNET HAD BEEN EXPLOITED.[1]

Cybersecurity due diligence is a complex and demanding activity with its own set of risks. Those risks need to be managed and should be conducted as an integral part of the process for any merger, particularly a merger that involves the integration of traditional and cloud-based environments (SaaS, PaaS, etc.), IoT, Big Data, data compliance (GDPR, PCI, etc.), or a company that has had a major security incident.

Several recent data breaches have revealed that cybersecurity risk arose in the post-acquisition and integration phase of the M&A process. Unfortunately, in some instances of breaches, executives didn't? realize that existing vulnerabilities can provide hackers unauthorized access to the seller's internal systems, exposing sensitive customer or proprietary data. Although these risks originate at the company being purchased, they are transferred to the new parent company. These acquiring companies might have avoided potentially significant legal fees and compliance fines if they had conducted a thorough cybersecurity due diligence assessment during the M&A process.

BASED ON 2018 STUDIES, THE AVERAGE COST OF A DATA BREACH GLOBALLY IS UP 6.4% YEAR-OVER-YEAR. IN ADDITION, THE AVERAGE COST FOR EACH LOST OR STOLEN RECORD CONTAINING SENSITIVE AND CONFIDENTIAL INFORMATION IS ALSO UP 4.8% AND CONTINUES TO TREND UPWARD.[2]

1. https://www.zdnet.com/article/telstra-discovers-pacnet-security-breach-after-takeover/
2. https://www.ibm.com/security/data-breach

$3.86M

Average price of a small-scale data breach involving 2,500 to 100,000 stolen records

$40M

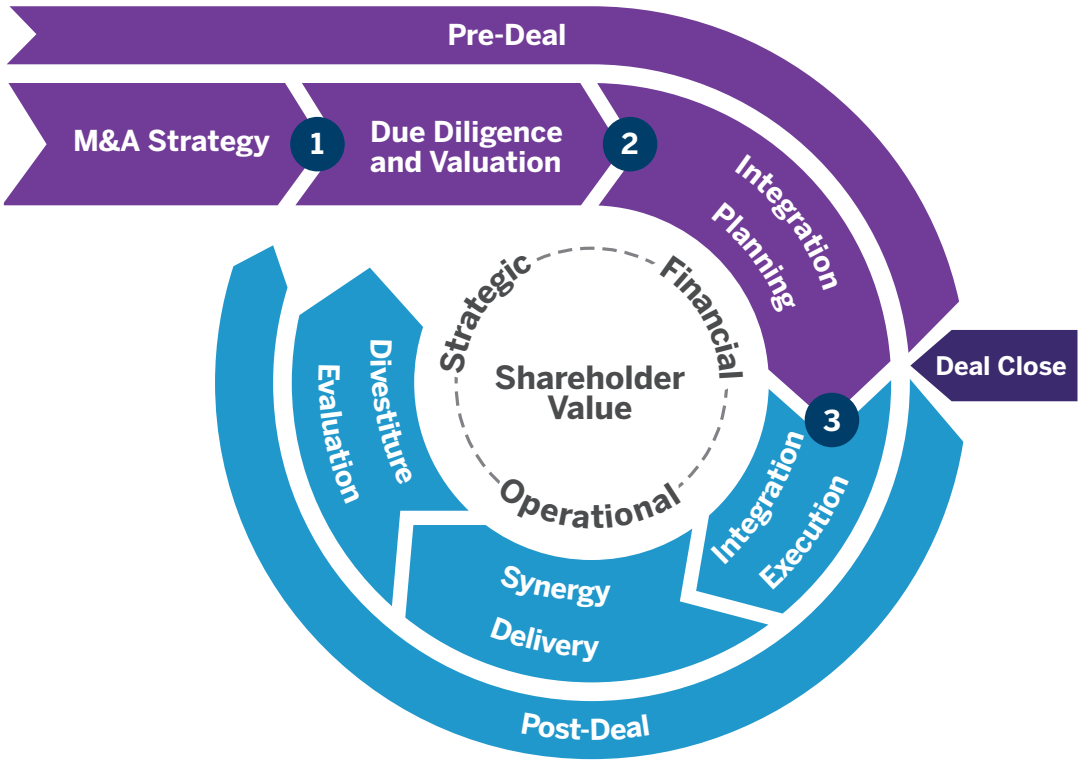
Potential cost of a mega-breach that compromises one million records

$350M

Approximate cost if a company suffers the loss of 50 million records

FTI CONSULTING'S APPROACH

In light of impending security risks and the resulting impact on deal value, cybersecurity considerations should be gauged early in the deal lifecycle and should never be an afterthought. Sellers and buyers should embed cybersecurity as a key component of deal due diligence and incrementally progress through integration planning and execution to ensure expected synergy, value delivery and long-term risk management.



1

If any of the following scenarios are identified in the deal, cybersecurity diligence needs to be included as part of the scope:

- A cross-border transaction that warrants data compliance considerations;
- Company A with a traditional IT environment is acquiring Company B which has SaaS, PaaS or IaaS focus;
- Company A with traditional data warehouse/business intelligence capabilities is acquiring Company B which focuses on Big Data;
- Company A is acquiring Company B with IoT capabilities; or
- A history of any security incident(s).

The security profile of the combined entity needs to be considered and high-level recommendations provided so that integration planning and execution can follow.

2

Integration planning should emphasize an interim plan and a long-term plan based on the security profile of NewCo post-integration, and planning should involve:

- Developing a security strategy;
- Analyzing data requirements of the combined entity, including employee, customer and partner profiles, data sources, location of data storage, etc.;
- Assessing network and storage requirements;
- Assessing clean room and plan set-up needs based on privacy and compliance considerations;
- Evaluating any change in application profile and resulting security considerations;
- Assessing security incident history, response plan and status of remediation; and/or
- Developing cybersecurity testing plan, including external testing based on target profile of entities.

3

Cybersecurity activities during integration should be aligned to the overall interim and long-term milestones and consider the following areas:

- Establishing a governance model for managing cybersecurity;
- Implementing data governance;
- Implementing a clean room, as required;
- Executing communication/messaging and security training;
- Conducting internal and external security testing;
- Implementing network monitoring;
- Ensuring compliance with regulatory mandates; and/or
- Developing risk mitigation strategies for the entities.

CONCLUSION

The potential erosion of deal value resulting from cyber incidents is forcing business leaders to consider cybersecurity as a key component of the deal lifecycle. Risks need to be identified early in the lifecycle so that an effective mitigation plan can be developed and executed. Addressing cybersecurity risks will prove beneficial not only in cost avoidance but also in protecting a business's brand reputation and preventing customer attrition. Therefore, adequate investments need to be incorporated into all phases of the deal lifecycle to enable a proactive approach to cybersecurity.

CASE STUDY:

CYBERSECURITY DUE DILIGENCE FOR SEMICONDUCTOR CARVE-OUT

Situation

- Large semiconductor firm sought to carve-out and spin-off a major product line.

FTI Consulting's Role

- Retained by the buyer's private equity sponsor to conduct commercial due diligence and evaluate business plan, IP portfolio and product development roadmap.
- Performed carve-out planning, quality-of-earnings assessment, and financial and IT diligence, including cybersecurity.

Outcome

- Developed carve-out plan identifying risks and opportunities.
- Provided high-level analysis of cybersecurity risks resulting from the transaction and proposed mitigation plan.

Sid Malhotra
Senior Managing Director Merger Integration & Carve-outs
+1 832.704.3065
sid.malhotra@fticonsulting.com

Renjit Lal
Managing Director
Merger Integration & Carve-outs
+1 469.616.7419
renjit.lal@fticonsulting.com

David Best
Senior Director
Cybersecurity
+1 267.592.9005
david.best@fticonsulting.com

Baber Khan
Senior Director
Business Transformation
+1 832.859.2213
baber.khan@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT™