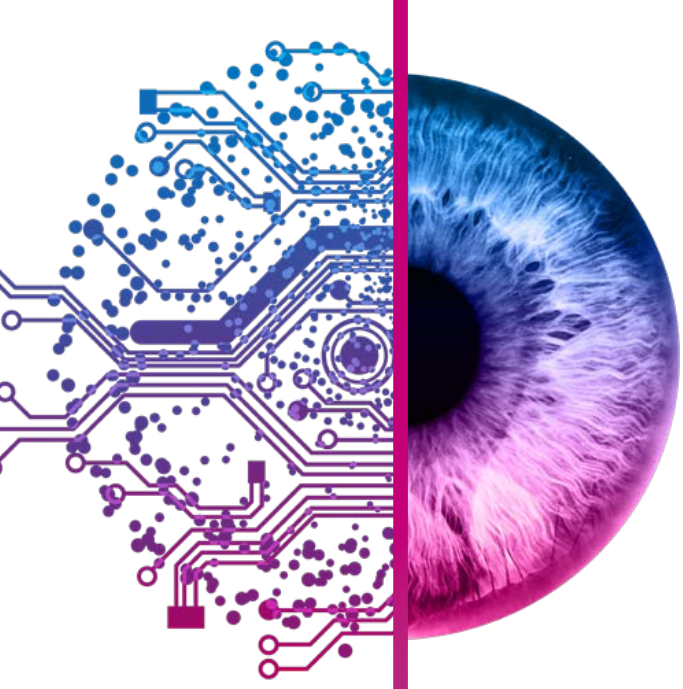


Allens › ‹ Linklaters

Data-Driven Business

Dealing with data: your M&A playbook

Tips for buyers and sellers and the five key questions to ask yourself to assess data opportunities and risks.

Over the past 18 months, we've seen data play an increasing role in M&A.

There is more M&A activity involving data rich assets, and – across all sectors – data opportunities and risks are impacting headline price, post-completion deal value and risk-allocation profile of investments and M&A transactions

Dealing with data in this context presents a number of challenges. **A shifting regulatory landscape** can make it tricky to assess the legitimacy of current (and proposed) data use cases, there are **complexities in appropriately valuing data**, and then there are the **practical challenges of extracting, sharing and protecting data.**

To maximise deal value, participants on both sides of the table are increasingly being called upon to accurately assess both the opportunities and risks of data. The failure to get it right can result in significant value erosion.

For both buyers and sellers, this playbook helps in-house counsel and dealmakers navigate the data issues that arise in mergers, acquisitions, demergers and investments to maximise value in these transactions.

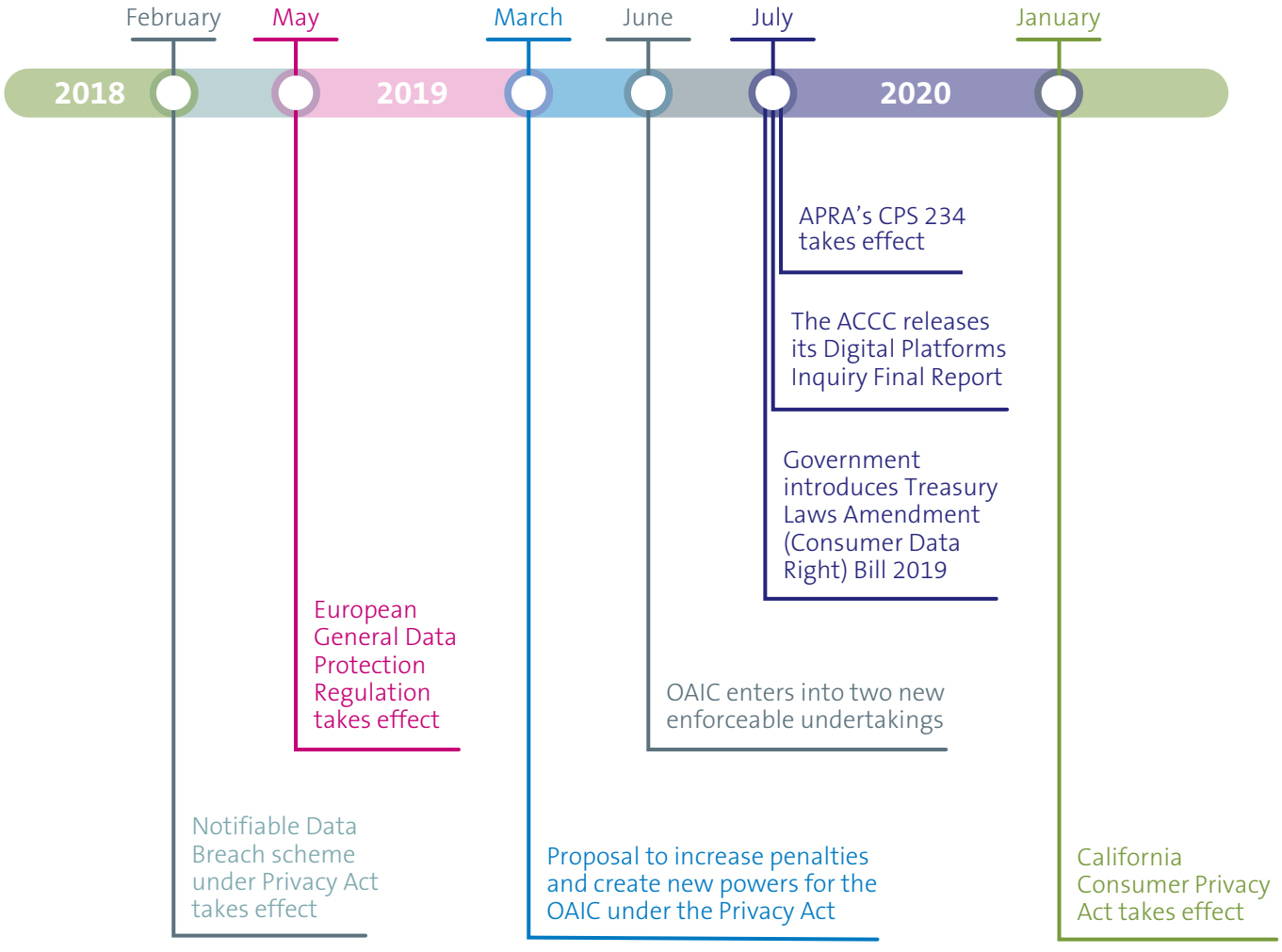
THE FIVE KEY QUESTIONS TO ASK WHEN ASSESSING DATA OPPORTUNITIES AND RISKS

1 HOW WILL THE REGULATORY LANDSCAPE AFFECT THIS TRANSACTION?

It is now more challenging than ever to evaluate the compliance of current and proposed data handling practices thanks to the volume and complexity of recent data regulatory developments in Australia and abroad.

Getting this right is essential, as both privacy and other regulators (which in Australia include the OAIC, ACCC, ASIC, APRA and FIRB) are increasingly scrutinising data handling and cybersecurity practices, and using their expanding enforcement arsenal to hold organisations to account in unprecedented ways.

Over the past 18 months



What should you do?

1. Sellers should uplift compliance prior to sale and demonstrate a sophisticated approach to data handling by evidencing the governance and compliance processes they have in place.
2. Buyers should have a sound understanding of the shifting regulatory landscape, the target's data flows and existing data use cases, and the circumstances of data collection and use (ie how was the data obtained? What consents were obtained? Who has the relevant rights to access and control data?) This will help buyers verify that:
   - the target's existing practices are compliant; and
   - any proposed new use-cases for the data (eg to inform new business lines, create targeted advertising or commercialise/ sell datasets) are legal.

   Being able to rely on existing customer consents, rather than procuring new consents or opt-ins, can be the difference between a successful product rollout with high adoption rates and an unsuccessful one. It is also far easier to design data use cases knowing the constraints, rather than having to retrofit compliance. Any necessary compliance uplifts should form part of a buyer's ongoing roadmap.

BEING ABLE TO RELY ON EXISTING CUSTOMER CONSENTS ... CAN BE THE DIFFERENCE BETWEEN A SUCCESSFUL PRODUCT ROLLOUT WITH HIGH ADOPTION RATES AND AN UNSUCCESSFUL ONE

2 WILL SHARING DATA IN THIS TRANSACTION CREATE COMPETITION ISSUES?

With the ACCC taking an increasingly bullish approach to cartel enforcement, parties need to consider whether sharing data pre-completion could constitute 'gun jumping' and risk breaching the prohibitions on cartel conduct. The ACCC recently published a guideline on gun jumping risks for merger transactions after bringing its first action for gun jumping against healthcare logistics company Cryosite.[1]

In addition, regulators are looking at data aggregation when assessing the likely competitive impact of transactions in merger clearance processes. The ACCC recently considered the aggregation of data when reviewing the proposed acquisition of a majority interest in the WestConnex toll-road project by a consortium led by Transurban. In that instance, the ACCC cleared the transaction subject to the consortium publishing particular traffic data to assist prospective bidders to compete for future toll-road concessions.[2]

PARTIES NEED TO CONSIDER WHETHER SHARING DATA PRE-COMPLETION COULD CONSTITUTE 'GUN JUMPING' AND RISK BREACHING THE PROHIBITIONS ON CARTEL CONDUCT.

1 The ACCC brought proceedings against Cryosite Limited in July 2018, alleging Cryosite had engaged in cartel conduct by entering into an asset-sale agreement with Cell Care, which required Cryosite to refer all sales and enquiries to Cell Care post-signing but pre-completion. Cryosite admitted to engaging in cartel conduct and was ordered to pay a $1.05m penalty. See the ACCC's press release here.

2 See the ACCC's press release here.

What should you do?

1. Do not share competitively sensitive information (including information relating to pricing, costs, business strategy, customer data and product innovation) beyond what is required for due diligence and integration planning.
2. Establish a protocol for information sharing, populating the data room and planning for post-merger implementation. It should be agreed what information is considered competitively sensitive or proprietary and should be withheld or only disclosed in a black box, and what information cannot be disclosed due to confidentiality obligations. Relevantly:
   - competitively sensitive information and data should only be disclosed to a select group of persons within the other party (a 'clean team'), who should not also be involved in making commercial decisions for the business;
   - it is preferable that competitively sensitive information and data only be disclosed on an aggregated basis; and
   - parties should consider whether particularly sensitive information and data should only be disclosed to third party advisors and legal counsel.
3. Operate independently until completion. Parties must continue to operate separately and make independent decisions about their conduct in the market until completion. In addition to sharing sensitive information, other pre-closing conduct which can constitute gun jumping includes taking steps to exercise control over the target, agreeing to cease supply or close business units and facilities, referring customers to the other party, establishing joint pricing or marketing policies and holding out that the companies have merged. Parties should seek advice on any pre-completion contractual obligations or notification requirements and ensure these do not confer control over the target.
4. Consider the competitive impact of aggregating merger parties' data assets when engaging with competition merger clearance processes.

WHAT CONSTITUTES GUN JUMPING?

- sharing **sensitive information**
- taking steps to **exercise control over the target**
- agreeing to **cease supply** or **close business units and facilities**
- **referring customers** to the other party
- establishing **joint pricing** or **marketing policies**
- **holding out** that the companies have merged

3 WILL FIRB APPROVAL BE REQUIRED?

FIRB has been intensifying its scrutiny of data handling practices as part of its approval process, resulting in:

- a more protracted, expensive and unpredictable approval process where the investment or acquisition involves access to data about Australians or access to critical infrastructure;
- increased interrogation by FIRB, as well as audits into the management and handling of data by the Australian Signals Directorate (ASD) (with little clarity around what the ASD is auditing or the outcome of those assessments); and
- the imposition of data security conditions, including restrictions on who may access acquired data and a requirement that data remain stored in Australia.

What should you do?

1. Prepare for a protracted (and consequently costlier) FIRB approval process – particularly where the investment or acquisition involves access to critical infrastructure or to data about Australians.
2. Consider including more detailed conditions precedent in the purchase agreement to address the allocation of risk and associated cost in relation to any FIRB conditions.
3. Ensure you understand and can evidence your data protection and data handling practices, as those practices and procedures will be the subject of intense scrutiny.
4. Negotiation of FIRB conditions is possible (within reason) and it is important to test and articulate the practical implications of these conditions and how they interact with existing regulation.

A GLOBAL TREND – THE GRINDR EXAMPLE

FIRB's increasing scrutiny of data handling by foreign entities is consistent with the approach being taken by similar regulators overseas. The Committee on Foreign Investment in the United States requested Chinese gaming and technology company Beijing Kunlun Tech sell the dating app Grindr after it acquired the company in 2018. The request demonstrates regulatory concerns that foreign ownership of sensitive data sets could be considered a threat to national security, particularly where there is the potential for foreign owners to blackmail officials or members of the public.

4 WHAT SHOULD WARRANTY AND INDEMNITY PACKAGES LOOK LIKE?

The market has shifted over the past two years, and it is now common practice for warranty packages to comprehensively address data, privacy and security matters.

With the growing prevalence of warranty and indemnity insurance, it is also critical for a buyer to demonstrate it has carried out genuine and thorough due diligence on data security and privacy arrangements to ensure insurance coverage will extend to such warranties.

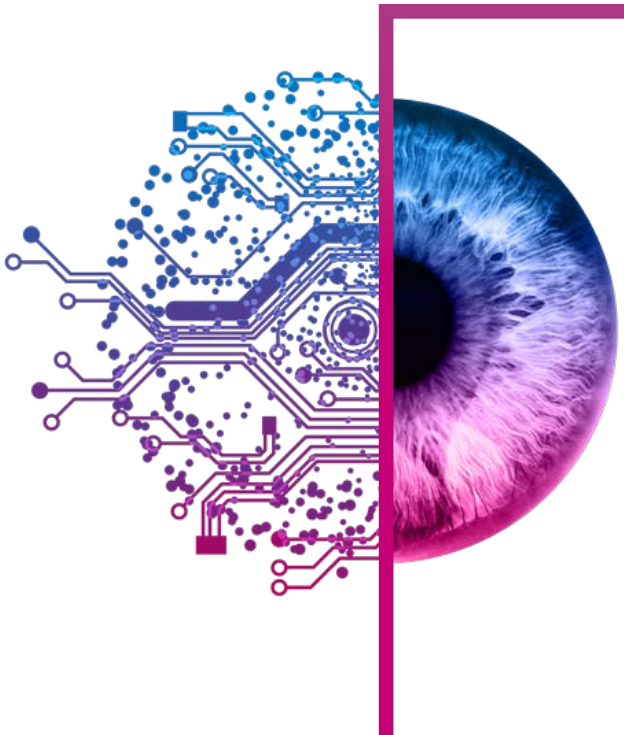
IT IS CRITICAL FOR A BUYER TO BE ABLE TO DEMONSTRATE IT HAS CARRIED OUT GENUINE AND THOROUGH DUE DILIGENCE ON DATA SECURITY AND PRIVACY ARRANGEMENTS

Of course, even the most robust warranties may not provide a satisfactory remedy if a material data incident has occurred. Assuming damages for breach of warranty are recoverable at all, they may not adequately compensate a buyer for the financial and reputational impacts such an incident will have on the acquired business.

Nevertheless, a comprehensive warranty package can be a useful diligence tool – flushing out disclosure of contingent privacy and data-related liabilities – which can make all the difference when it comes to assessing whether a transaction is high-risk and/or gaining leverage in purchase price negotiations.

What should you do?

1. Buyers should seek comprehensive data, privacy and security warranties, eg that:
   - there has been no unauthorised access to systems/data during a reasonable lookback period;
   - industry best practice steps have been taken to ensure system security;
   - the target's business is compliant with data protection laws; and
   - there have been no proceedings, investigations, complaints or notifications regarding data or privacy matters.
2. Sellers should be prepared to be asked for these warranties and should have a plan for how and when to disclose any material privacy regulatory issues or security incidents to ensure these matters do not have a material impact on buyer interest, deal value or leverage.



5 WHAT PRACTICALITIES NEED TO BE ADDRESSED TO ENSURE BUSINESS CONTINUITY AND AN ORDERLY TRANSITION AND SEPARATION?

Understanding:

- a target's IT infrastructure;
- how data will be separated, shared and protected;
- how data migration will occur; and
- how interrelated systems will be transitioned,

is critical to ensuring business continuity for buyers and sellers post-completion.

Add to the mix a patchworked IT infrastructure, potentially with various points of connectivity (such as IoT devices), configuration weaknesses and multiple commingled data sets, and the picture becomes even more complex.

Grappling with these issues (both from an IT and commercial standpoint) can be extremely time-consuming and is often left until the eleventh hour, causing unnecessary deal pressure and delay.

What should you do?

1. Understand the separability of systems and datasets. Parties should ask themselves:
   - which entities will need access to what data?
   - how will the parties securely separate, extract and convert data while retaining its integrity?
   - who is going to undertake this work and at whose cost?
   - once data has been shared, how will the parties maintain confidentiality over that data in the absence of proprietary rights? and
   - if both buyer and seller will share the same datasets, how will each party control what the other party can do with such data (eg cross marketing)?
2. Properly address these matters through diligence and by negotiating data handling and transitional services agreements. Keep in mind that:
   - complexity means it is usually more efficient to arrange a call with the appropriate individuals from the seller in order to address these issues rather than sending RFIs back and forth or relying on documentary disclosures; and
   - it is vital the agreement in place between the buyer and seller does not create any vulnerabilities during the transition, which may expose the buyer to liability.

ADDRESS THE DATA SEPARATION ISSUES EARLY AND WITH THE RIGHT PEOPLE

3. Consider data sharing requirements during transition. Participants will also need to determine what (if any) data sharing will need to occur during the transitional services term, and possibly beyond that time as part of a strategic alliance arrangement. Buyers may need to build or license tools and APIs to enable data migration.
4. Align approach to notifications and consents. Participants will need to ensure early alignment in assessing whether and how consent to the collection, use and disclosure of personal information needs to be obtained from relevant individuals or notifications provided to those individuals. This can be difficult when there are differences in risk tolerance or approach to these matters as between the participants.
5. Buyers should use the transaction as an opportunity to:
   - improve business efficiency;
   - rectify issues identified during due diligence; and
   - lay the groundwork for future business growth.

SPOTLIGHT ON CYBERSECURITY

MORE EXPENSIVE THAN THE MINI BAR: THE MARRIOTT EXAMPLE

When Marriott International Inc acquired Starwood Hotels & Resorts for USD13.6 billion in 2016, it also acquired a huge problem in the form of an unsecure (and, it turns out, compromised) guest reservation database. The data breach affected Starwood guests across the globe, whose personal information - including names, addresses, date of birth, gender, passport numbers, rewards information, arrival and departure information, communication preferences and credit card numbers - were contained within the database. Not surprisingly, the consequences for Marriott were swift and severe:

THE COST OF OVERSIGHT

- **5.6%** share price hit
- **£99** million fine from the UK ICO
- **multiple** class actions
- regulatory **scrutiny**
- remediation **costs**
- calls to **foot the bill** for costs incurred by affected individuals
- **reputational damage**

Although unauthorised access to the Starwood database was first detected in September 2018, the breach appears to date back to 2014, before Marriott's acquisition.

HAD MARRIOTT CONDUCTED ADEQUATE DUE DILIGENCE, THE ENTIRE SITUATION MIGHT HAVE BEEN AVOIDED.

We see businesses forensically interrogate the financial and regulatory risks of targets. Yet when it comes to data security risks, buyers often do little more than ask whether the target is aware of any previous data breaches. If a buyer was looking to acquire an asset in the manufacturing sector, a thorough environmental impact assessment would be conducted and to diligence licensing arrangements at manufacturing sites. The same approach should be taken for data security risks, particularly given data is now a critical asset of most companies.

What is at stake?

It is important to adequately diligence a target's security posture and historic vulnerabilities, considering how buyers tend to react when cybersecurity issues come to light.

There are plenty of examples of buyers shaving significant value off a purchase price (or walking away altogether) when it becomes known a prospective target has suffered a data breach. Take, for instance, Verizon's US$350 million reduction in the purchase price it paid for Yahoo's internet business in 2017 after an earlier data breach came to light.[3] Another example was the significant valuation discount (30%, or approximately $20bn) when Softbank invested in Uber in January 2018. That valuation discount was attributable, among other things, to Uber's 2016 data breach incident.[4]

3 Vindu Goel, 'Verizon will pay $350 million less for Yahoo', New York Times (21 February 2017).
4 CNBC article discusses the 30% discount on purchase price but not link the drop in price to the hack, 'SoftBank agrees to buy large stake in Uber' (28 December 2017)

of companies surveyed had encountered a critical cybersecurity issue during an M&A deal that had put the deal in jeopardy.[5]

of directors said the occurrence of a high-profile data breach at an acquisition target would deter them from completing the transaction altogether.[6]

of directors claimed that while they might not be completely deterred, a data breach would significantly lower the valuation.[7]

Where a breach is detected post-completion, there is also a risk the buyer will be being forced to bear the cost of legal claims brought against the target, regulatory action/fines and reputational damage. According to a Forescout survey, 65% of respondents had experienced buyers' remorse post-deal due to cybersecurity issues that had emerged.[8]

Where to from here?

There needs to be a cultural shift towards the recognition of data security as a significant threat to transaction value and deliverability.

Buyers need to become accustomed to assessing data and systems security risks with the same rigour with which they analyse other business risks. And this should be happening in all sectors – not just those that are consumer facing, or that were traditionally considered to be technology or data-driven.

DATA SECURITY SHOULD BE A FOCUS FOR ANY ORGANISATION THAT HAS TRADE SECRETS, CONFIDENTIAL INFORMATION OR THAT IS RELIANT ON CRITICAL IT SYSTEMS.

Buyers should ensure they fully understand the security posture and cyber resilience of targets, including the adequacy of protections (including within its supply chain) that the business has implemented to protect its systems and data, its history and management of data breaches, and its cybersecurity governance arrangements. Any cybersecurity risks should then be addressed in the valuation and warranty package.

As buyers become increasingly alert to the risks of inadequate data security, sellers will also have a vested interest in ensuring there are adequate systems in place for managing those risks to maximise deal value and minimise post-completion complications.

5 Forescout - The Role of Cybersecurity in Mergers and Acquisitions Diligence.
6 Cybersecurity and the M&A Due Diligence Process: A 2016 NYSE Governance Services/Veracode Survey Report (2016).
7 Cybersecurity and the M&A Due Diligence Process: A 2016 NYSE Governance Services/Veracode Survey Report (2016).
8 Forescout - The Role of Cybersecurity in Mergers and Acquisitions Diligence.

TIPS & TRICKS

TIPS FOR SELLERS

The following will help you 'get your house in order' in advance of the transaction process, with a view to getting buyers comfortable with any data-related risks and maximising the purchase price:

1. **Map the data flows.**
   Be able to demonstrate a clear understanding to prospective buyers of a target's data flows. This is key to communicating the potential use-cases for data and extracting maximum value for the divested business.

2. **Ensure privacy compliance.**
   Be able to demonstrate a sophisticated understanding of the privacy regulatory framework affecting the target's business and how this has been complied with. Be prepared to explain how key consents have been obtained, how regulations have been addressed and what executive oversight exists over privacy matters. Something as simple as an out-of-date privacy policy can send a clear message that a target is not on top of these issues.

3. **Review third party arrangements.**
   Ensure they are legally compliant and contemplate comprehensive data handling arrangements. You should also be prepared to answer questions regarding what due diligence and audits are carried out on the target's supply chain. This will reassure buyers that the target's third party arrangements do not represent potential points of vulnerability or liability going forward.

4. **Manage your cyber risks.**
   Being able to demonstrate a sophisticated understanding of cybersecurity risks and their potential impact on the target's business will provide prospective buyers with comfort not only that the target is well placed to withstand potential threats, but also that it is less likely to have suffered a historic breach which has not yet been uncovered. You should ensure a mature and comprehensive cybersecurity risk-management program has been implemented, including documenting and testing data breach and/or cyber incident response and recovery plans.

5. **Know what skeletons are in the closet and have a plan for disclosure.**
   Be prepared to discuss any previous or ongoing privacy claims, cybersecurity incidents and data breaches, and be willing to divulge information such as the impact on the business, how long it took to discover the incident, how it was managed, what data was affected, any information known about the attackers and affected individuals and engagement with law enforcement and regulators. Ultimately, some attacks or breaches are unavoidable and need not scare off buyers if they were appropriately managed.

TIPS FOR BUYERS

Identifying both the value of the data assets of a target and any risks, will provide a greater ability to outbid other potential investors and recognise data revenue opportunities post-investment.

1. Prioritise data diligence.

The market is not yet as sophisticated at disclosing information about data assets and use (or identifying associated liabilities) as it is for 'traditional' tangible assets. This means you will generally need to be more proactive than usual in trying to understand:

- **The nature of the data assets** – including what are the crown jewels? What are the data flows into, within and outside the organisation? Where are the key datasets located, who has access and how are they stored and protected? How separable is the data? What can the organisation do with the data (technically and legally)? How is the data used (eg the nature of any targeted advertising, data analytics or commercialisation, data purchase/sharing/matching activities etc)?
- **Information regarding data governance arrangements** – including the target's organisational data governance structure, internal data handling policies, copies of external privacy policies and consents, Privacy Impact Assessments or similar reports and data breach notification plans.
- **Cyber resilience** – including the key risks to a target's systems and data and what steps have been taken to help manage those risks if they were to eventuate. This is not only relevant to evaluating information-security risk but also the risk of business interruption (whether that be the result of a cyberattack, a natural disaster or otherwise). You should request:
  - details of any known or suspected data or information security breaches or malfunctions suffered either by the target or its service providers, and how they were managed;
  - details of the target's approach to ensuring the security of its third-party suppliers (both at the time of onboarding as well as subsequent monitoring and audits);
  - particulars of the technical, physical and organisational security measures used to protect hardware, software and data – including IT-related measures, copies of Cyber Security Impact Assessments, penetration tests or similar IT audits (eg PCI DSS audits and/or ISO 27001 assessments); and
  - details regarding the scope of cyber-insurance coverage and any claims.
- **The opportunities** – including what are the gaps in the data and what more could you do with it? Is there value in commercialising the data, or in otherwise using or enriching the data to facilitate decision making, inform new business lines or create targeted advertising? It is important to understand the regulatory framework that surrounds the data as well as the IT-systems limitations.

THERE IS NO POINT HAVING A DETAILED PLAN FOR HOW DATA WILL BE USED IF IT CAN'T BE ACHIEVED IN PRACTICE

- **The key risks** – including to test whether the data is as valuable as anticipated. Can you make use of it in the way you want, or would regulatory or contractual restrictions hamper this use? Might there be major reputational damage or remediation costs caused by earlier non-compliance with regulation or a data breach?

1. Engage early and with the right people.

According to Forescout's 2019 cybersecurity report, only 36% of respondents strongly agreed that their IT team is given adequate time to review a target's cybersecurity standards, processes and protocols before the deal is completed.[9] Relying on written responses to RFIs will generally not be sufficient or appropriate when it comes to understanding data handling arrangements. Where possible, diligence should include discussions with the executives responsible for data and security matters (such as the target's General Counsel, Chief Technology Officer, Chief Information Security Officer, Chief Information Officer and Privacy Officer), covering both legal and functional enquiries.

2. Address data separation and sharing arrangements.

It is important to deal with the practicalities of data separation and ongoing sharing arrangements, both through diligence and by negotiating data handling and transitional services agreements that properly address these matters.

3. Don't assume warranties are the solution.

Seek a comprehensive warranty package to flush out disclosure of contingent privacy and data-related liabilities, keeping in mind that even the most robust warranties may not provide a satisfactory remedy if a material data incident has occurred.

4. Foreign buyers should prepare for a protracted FIRB approval process.

As data security becomes a growing area of concern for many, FIRB is becoming increasingly invested in how foreign investors handle data and is imposing data security conditions to protect national security and safeguard Australians' personal information.

5. Take advantage of the opportunity to start afresh.

The post-completion phase offers an opportunity to reset and consider how the acquired business' data practices can be integrated with your own. Taking the time to properly review and update these practices post-acquisition and uplift data governance practices will set you up to extract the most value from the companies you acquire, as well as ensuring the long term integrity of your business.

CONTACTS

Gavin Smith
Partner, Head of Technology, Media and Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au

Valeska Bloch
Partner
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Michael Morris
Partner
T +61 7 3334 3279
Michael.Morris@allens.com.au

Michael Park
Partner
T +61 3 9613 8331
Michael.Park@allens.com.au

Ian McGill
Partner
T +61 2 9230 4893
Ian.McGill@allens.com.au

Mark Malinas
Partner
T +61 3 9613 8485
Mark.Malinas@allens.com.au

Jacqueline Downes
Partner
T +61 2 9230 4850
Jacqueline.Downes@allens.com.au

Chris Blane
Partner
T +61 2 9230 4298
Chris.Blane@allens.com.au

Phil O'Sullivan
Managing Associate
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au

David Rountree
Managing Associate
T +61 2 9230 4773
David.Rountree@allens.com.au

Jessica Mottau
Managing Associate
T +61 2 9230 4587
Jessica.Mottau@allens.com.au

Elyse Adams
Managing Associate
T +61 3 9613 8534
Elyse.Adams@allens.com.au

Dominic Anderson
Senior Associate
T +61 2 9230 4099
Dominic.Anderson@allens.com.au

David Mierendorff
Senior Associate
T +61 2 9230 4038
David.Mierendorff@allens.com.au

9 Forescout - The Role of Cybersecurity in Mergers and Acquisitions Diligence.

allens.com.au/data*driven*business