Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell, Leah Schloss, Maury Riggan and Jason C Chipman

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Leah Schloss

Maury Riggan

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2019
For further information please contact Natalie.Clarke@lbresearch.com

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-223-7

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

RICHARD DENATALE

HUNTON ANDREWS KURTH LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its third edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Part I

A 'Typical' Cyber Investigation

7

Cyber and Data Privacy Due Diligence

Megan Gordon, Daniel Silver, Benjamin Berringer and Brian Yin[1]

Introduction

On 25 July 2016, Verizon Communications announced that it would pay US$4.83 billion in cash to purchase Yahoo! Inc.[2] Seven months later, that price was cut by US$350 million and Yahoo! agreed to pay 50 per cent of any costs relating to government investigations and private litigation relating to historic data breaches.[3] The reason for the change? Verizon identified a massive undisclosed data breach during its due diligence, which dramatically changed the value of the transaction.

The Yahoo! data breach highlights an increasingly important aspect of due diligence in today's data- and technology-driven society: cyber and data privacy due diligence. These topics, which were once peripheral to a transaction, have become critical. This chapter discusses some of the key issues that practitioners should consider when analysing a company's cybersecurity and data privacy practices, including pre-diligence steps, commonly requested diligence items and potential red flags that may signal the need for additional scrutiny.

Overview of cyber due diligence

A critical aspect of any transaction is due diligence. During this process, a purchaser or investor (the Buyer) will typically conduct an in-depth review of the corporation to be acquired (the Target) to accurately value the transaction. This due diligence will also form the basis of the representations and warranties that the Target will include in the transaction documents.

---

1 Megan Gordon and Daniel Silver are partners and Benjamin Berringer and Brian Yin are associates at Clifford Chance US LLP.

2 Verizon, 'Verizon to acquire Yahoo's operating business' (25 Jul 2016), https://www.prnewswire.com/news-releases/verizon-to-acquire-yahoos-operating-business-300303133.html.

3 Verizon, 'Verizon and Yahoo amend terms of definitive agreement' (21 Feb 2017), https://www.prnewswire.com/news-releases/verizon-and-yahoo-amend-terms-of -definitive-agreement-300410420.html. The revised agreement's cost-sharing provision excluded investigations by the Securities and Exchange Commission.

Preparing for diligence: diligence requests

Due diligence, including cyber due diligence, is not a one-size-fits-all exercise – the Buyer needs to have a basic understanding of the Target's business to focus on key issues. For example, if a Target only does business with other corporations, due diligence focusing on the protection of personally identifiable information (PII) and credit card information is less important than due diligence focusing on the protection of trade secrets. Conversely, trade secret diligence is probably less important for a consumer-facing Target that collects significant PII. As a result, Buyers should consider the nature of the Target and its data to properly scope and focus due diligence. The following are some of the issues to consider:

- Industry. In the United States, unlike in Europe, cybersecurity and data privacy are not subject to a single overarching regulatory and statutory framework. Instead, the requirements will vary depending on the specific industry. Therefore, for certain industries, such as healthcare and financial services, it is important that diligence questions focus on the requirements that are unique to those industries.
- Customer profile. Having a well-developed understanding of a Target's customer base prior to conducting due diligence is also important. By identifying the Target's typical customers (e.g., individuals, other corporations, the government), the Buyer can focus diligence requests on the typical data privacy and cybersecurity issues that arise in companies with the identified customer profile.
- Location. As discussed in more detail in Chapter 10, a Target located in the European Union or that does business with EU customers is likely to be covered by the General Data Protection Regulation (GDPR) and therefore should be subjected to more scrutiny given the large penalties that are authorised under the GDPR.[4]
- Data collection practices. Understanding the data that a Target typically collects and how it is collected will allow a Buyer to better understand the Target's data privacy and cybersecurity risks. Care should be taken in analysing any Target that collects a significant amount of PII or receives credit card information.
- Previous cybersecurity incidents. A review of historic cybersecurity incidents can help a Buyer understand whether a Target has system vulnerabilities or inadequate policies and procedures, which may indicate that there are unidentified risks related to the Target. Certain documents (such as policies and procedures) may warrant more scrutiny for a Target that has a history of cybersecurity breaches and other incidents, and in some cases the Buyer may want to engage in careful technical diligence of the Buyer's system.

These initial observations will serve two purposes. First, it will allow the Buyer to tailor its due diligence requests to the specific Target by identifying issues that are likely to be most important to the review. Second, it will allow the Buyer to identify at an early stage the biggest risks to the transaction and ensure that those risks are specifically analysed during the due diligence review. The following are some of the key risks that can be identified in the process:

4 A company that is found to have violated the General Data Protection Regulation are subject to penalties of €20 million or 4 per cent of the company's global annual revenue, whichever is greater. See Article 84, Regulation (EU) 2016/679 (the General Data Protection Regulation [GDPR]).

- Financial industry. Cybersecurity in the financial sector has been an increasing area of focus for US and state regulators. Therefore, cyber diligence should be a specific area of focus for these entities. This diligence should consider whether, for example, the financial institution complies with the New York Department of Financial Services (NY DFS) cybersecurity regulations,[5] the Federal Trade Commission's (FTC) Safeguard Rules,[6] the Securities and Exchange Commission's Regulation S-P,[7] Interagency Guidelines Establishing Information Security Standards or other provisions of the Gramm-Leach-Bliley Act (GLBA) relating to data privacy and security,[8] as applicable.
- Healthcare industry. Targets in the healthcare industry may be subject to laws that specify data protection requirements for that sector, such as the Health Insurance Portability and Accountability Act (HIPAA)[9] and the Health Information Technology for Economic and Clinical Health Act (the HITECH Act).[10]
- Government contractors. Government contractors are subject to a variety of cybersecurity requirements, the most prominent of which is the National Institute of Standards and Technology's (NIST) Special Publication No. 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).[11] Federal government contractors may be required to implement all (Department of Defense contractors and subcontractors) or some (all other federal agency contractors and subcontractors) of the requirements in this standard.

---

5 Among other requirements, the New York Department of Financial Services [NY DFS] cybersecurity regulations require that regulated entities carry out a risk assessment in accordance with written policies and procedures, which must include: (1) criteria for evaluation and categorisation of threats; (2) criteria for assessment of confidentiality, integrity security and availability of the DFS-licensed entity's information systems and non-public information; and (3) requirements describing risk mitigation or acceptance. Regulated entities must also maintain systems that are designed to reconstruct material financial transactions and keep audit trails designed to detect and respond to a cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operation of the entity. See NY Comp. Codes Rules & Regs Title 23, Section 500.

6 The Federal Trade Commission's [FTC] Safeguards Rule, a regulation adopted pursuant to the Gramm-Leach-Bliley Act, requires financial institutions to implement a written information security plan to protect customer information, which must include steps to protect against threats or unauthorised access to the information. See FTC Safeguards Rule, 16 CFR Section 314.

7 Regulation S-P requires covered entities to have policies and procedures to address the protection of customer information and records. Regulation S-P, 17 CFR Section 248.30.

8 The Interagency Guidelines Establishing Information Security Standards establish standards for administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and proper disposal of customer information. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (Board); 12 CFR Part 364, app. B (FDIC); and 12 CFR Part 570, app. B (OTS).

9 The Health Insurance Portability and Accountability Act [HIPAA] Security Rule and the HIPAA Privacy Rule require the adoption and maintenance of reasonable and appropriate administrative, technical and physical safeguards for protecting personal health data. See HIPAA Security Rule, 45 CFR Section 160, 164; HIPAA Privacy Rule, 45 CFR Sections 160, 164.

10 The Health Information Technology for Economic and Clinical Health Act [HITECH] Act strengthens the civil and criminal enforcement of HIPAA rules that protect health information transmitted electronically. See HITECH Act, 42 USC Section 300jj et seq., Section 17901 et seq.

11 See NIST, Special Publication No. 800-171, Rev. 1 'Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations' (7 June 2018), https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

- Companies that conduct transactions with credit cards. Any company that collects and processes credit card information is likely to be required to comply with the Payment Card Industry Data Security Systems (PCI DSS).[12]
- Companies with EU customers. The GDPR, which took effect in May 2018, is a sweeping EU data privacy law with broad extraterritorial effect that aims to protect the personal data of EU residents.[13]

Using this information, the Buyer can determine a materiality threshold for its diligence process. This materiality threshold is likely to take into account financial, litigation and reputational risk and reflect the Buyer's appetite for risk and the importance of the Target's data and IT assets to the value of the transaction overall. For example, diligence on a Target that collects significant PII is likely to have a lower materiality threshold for data breaches – which could cause significant litigation and reputational risks – than diligence on a Target that has little PII. Whatever the materiality threshold, it is important that the Buyer communicates this threshold to the diligence team as well as the Target. Furthermore, a Buyer should periodically re-evaluate the project's materiality threshold in light of changes in the value of the deal or information uncovered during the diligence process.

Once the Buyer has assembled this information, the next step in the process is to make information requests. These requests are aimed at allowing the Buyer to fully understand the Target's cybersecurity and data privacy policies. The goal is to ensure that at the end of the diligence process the Buyer has:

- analysed any pre-existing data breaches or other actual or threatened data security- or privacy-related enforcement or litigation;
- understood the PII that the company collects;
- identified sensitive data and data assets;
- evaluated the seller's cybersecurity infrastructure;
- analysed the adequacy of the Target's cybersecurity policies and procedures, including penetration testing, vulnerability assessments and corrective follow-up; and
- identified cyber-relevant terms of vendor and customer contracts, especially with respect to any indemnification provisions relating to cyber incidents.

As has been discussed, these requests should consider information that the Buyer already has about the Target. For example, if the Target is a financial institution, these requests will need to address the specific documents that the Target is required to have under the NY DFS regulations and the GLBA Safeguards Rule and Interagency Guidelines.[14] Similarly, diligence on a government contractor should request documents establishing compliance with NIST and

12 The Payment Card Industry Data Security Systems [PCI DSS] applies to all companies that store, process or share cardholder data and consists of technical and operational practices required for systems that store and use this data. See Payment Card Industry Security Standards Council, Data Security Standard: Requirements and Security Assessment Procedures, Version 3.2.1 (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf (note: users may first need to accept Ts & Cs of website).

13 Regulation (EU) 2016/679.

14 e.g., the NY DFS cybersecurity regulations requires covered entities to have: written policies approved by the board of directors that describe the cybersecurity programme in place to protect consumers' private data; records of risk assessments; audit trails; and various notices and certifications submitted to the superintendent.

other government-mandated standards. On the other hand, requests to Targets that process credit card transactions may focus on PCI DSS requirements.[15]

In addition to these targeted requests, the Buyer should also ask for information about any historic data breaches, enforcement matters or litigation; the Target's cyber policies and practices; copies of any existing documents describing the Target's compliance with applicable laws; documents describing any third-party testing of the Target's cybersecurity and data privacy practices; and any other existing documents describing the Target's cyber policies and practices. The Buyer should also consider whether the Target currently has cybersecurity insurance. As diligence is conducted, observations and findings should be cross-referenced, where possible, against both the Target's documents and industry standards. Any discrepancy will be noteworthy, not necessarily as a red flag, but as a subject that requires further diligence to ensure that the deviation does not affect the Target's valuation or raise concerns about potential future liabilities.

Conducting the diligence: policies and procedures

Cyber and data privacy policies and procedures are critical documents to review during due diligence. Depending on the Target, there may be a variety of policies and procedures relating to these topics, including policies regarding data access and confidentiality, data retention, cyber incident response, disaster recovery, rights of data subjects, data disclosure and sharing, data confidentiality, acceptable use of company-issue devices and the use of social media.

These policies and procedures come in a wide variety of forms. Some Targets may have separate policies that are internal-facing and external-facing; for example, a company may have a privacy policy that is published on its website as well as a more detailed internal privacy policy in the company handbook. There may also be different policies and procedures for data of different data subjects; for example, a company may have separate retention policies for existing customer data, prospective customer data and employee data. Similarly, a Target company comprised of multiple divisions or units carrying on separate businesses may have different policies and procedures that need to be analysed separately. These variations are immaterial, so long as the Target has policies and procedures in place that, as a minimum, are reasonable and comply with the Target's contractual and legal obligations.

The Buyer should have a checklist of the policies and procedures that they expect to see prior to beginning this review. This checklist will be informed by the Buyer's pre-diligence analysis regarding the Target's industry, the types of data that are likely to be held and the Target's customer profile. Using that checklist, the Buyer should aim to make, as a minimum, the following determinations about those policies and procedures.

Do the policies and procedures exist?

Lack of policies is typically a significant red flag that may warrant re-evaluating the Target's purchase price and, as a minimum, is likely to require disclosure in any purchase agreement.

15 The PCI DSS consists of 12 broad requirements that make up six groups entitled 'control objectives'.

Are the policies and procedures adequate?

This evaluation should consider not only relevant laws and regulations but also industry best practices, contractual obligations and public representations (e.g., whether internal policies and procedures align with public-facing privacy notices or past statements on the Target company's data practices). Attention should be given to Targets that are in one of the US industries, such as healthcare, that are subject to higher data protection standards. As part of this process, the diligence team should also review historical policies and procedures to determine whether there is any legacy risk of complaints or violations.[16] The evaluation should further consider whether the policies and procedures are based on a comprehensive risk assessment of the company or appear to be off-the-shelf policies that do not address the Target's risk profile.

How does the Target collect and store PII?

Increasingly, one of the biggest risks that corporations face is a data breach that exposes customer PII. Therefore, diligence needs to ensure that the Target is only collecting PII with customer consent (where required), that the Target is taking steps to delete unnecessary historical PII and that the Target is using appropriate safeguards to store the PII. In this regard, it is important to note that most Targets will have at least some compliance obligations under the GDPR, which includes specific requirements about policies and procedures. Therefore, as part of this review, the Buyer must ensure that the Target has policies in place that fulfil those requirements.

What steps does the Target take to protect special categories of sensitive data?

Specifically, the Buyer should ensure that the Target has taken reasonable steps to protect any special categories of sensitive data (such as healthcare or financial data) that it holds from unauthorised internal or external access. As part of this process, the Buyer should also evaluate how the seller has identified special categories of sensitive data and whether this identification is over- or underinclusive.

As part of its review of policies and procedures, the Buyer should also request related documents, such as cyber-focused risk assessments, testing records and training logs. These records can serve a variety of purposes; for example, risk assessments may help to identify areas of concern and vulnerability, or help to identify and mitigate legacy risks. Similarly, penetration testing and employee training records, audits and other evaluations can identify any specific historic problems at the Target and provide insight into the attention (or lack thereof) the company has historically paid to cybersecurity and data privacy issues.

Once the Buyer has completed its review of the Target's policies and procedures and related documents, it will need to consider whether and how any red flags that have been identified can be mitigated. One of the most common data privacy and cybersecurity representations that is included in a purchase agreement is that the seller or Target has adequate policies and procedures relating to its processing of personal data and that these policies comply with

16 There are no general laws in the United States that require such records to be maintained. However, failure to maintain these records may be a red flag, depending on the standards and best practices of the Target company.

applicable laws and regulations, as well as any other obligations the company may have from service agreements, industry standards, or public-facing disclosures and communications. A less common representation may go further and state that the seller has made all current and past versions of its policies and procedures available to the Buyer. To the extent that due diligence findings do not support these representations, the Buyer should ensure that these issues are included on any disclosure schedule.

Cyber diligence: historical exposure to cybersecurity and data privacy incidents

Understanding historical cyber and data privacy events is also a major area of focus in due diligence.

First, the Buyer needs to understand whether there are any pre-existing risks from an earlier breach or whether there are undisclosed breaches.

Second, the Buyer needs to recognise that companies are increasingly vulnerable to consumer complaints about how their data is handled. For example, the GDPR gives all data subjects in the European Union the right to file a complaint with an empowered regulatory authority or to bring a private suit against companies who do not honour their rights.[17] The United States has lagged in this regard, but it is catching up quickly with state laws such as the California Consumer Privacy Act and increasing popular support for a federal law.[18]

In this environment, Buyers need to understand the risks of past or future data breaches to value adequately the potential liability that they are acquiring from the Target, as well as the steps that the Buyer can take to mitigate that liability. This diligence typically includes evaluating any complaints against the company (including notices of violations and investigations) by individuals and regulatory authorities. The cyber diligence team should also review any incident logs that are available, because the frequency of cybersecurity incidents (whether successful or not) can provide insight into whether the company and its data systems are common targets. Diligence should also include public records searches to identify whether the Target has been subject to any relevant allegations regarding cybersecurity. In addition, this review should be informed by the processes and procedures through which the Target detects, monitors and responds to cybersecurity incidents.

The Buyer should also consider complaints and notices of violations relating to other data privacy issues, such as the failure to respect a data subject's access rights or non-compliance with restrictions on data sharing. The existence of such complaints may identify an undisclosed liability, while the frequency of violations and complaints can inform the Buyer about the customers (and other data subjects) it is acquiring with the Target. Finally, the Target's response to such incidents can be a useful data point for understanding the Target's culture of compliance with cybersecurity and data privacy requirements.

Once the diligence review is complete on this area, the Buyer can protect itself from undisclosed liabilities by adding robust representations and warranties to the purchase agreement. A representation that the Target is not aware of any cybersecurity or data privacy

17 Article 77, GDPR.

18 In 2018, California adopted the California Consumer Privacy Act, which featured many requirements similar to those of the GDPR, including the right to file a private action. 2018 Cal. Legis. Serv. Ch. 55 (West). As at April 2019, there is not yet any federal law that broadly provides such a right, but it would not be surprising to see such a provision in a future national data privacy law.

incident (whether successful or not) will provide comfort to the Buyer that it understands the risks before the purchase is finalised. It is important to understand, however, that this representation does not protect against undetected breaches or unknown complaints. In addition, in some circumstances sellers may insist that these representations are limited by a specific look-back period, such as three or five years. This is one reason why thorough diligence on a company's policies and procedures is so important – a company with a culture of robust cybersecurity policies and effective monitoring is less likely to have undiscovered issues.

Conducting diligence: contractual obligations and liabilities

Another area the Buyer should consider is whether the Target has contractual cybersecurity obligations. There are two types of contractual relationships that may touch on cybersecurity and data privacy – contracts with service providers and contracts with customers – both of which can create obligations and liabilities that extend beyond those imposed by laws and regulations.

In the United States (and most other jurisdictions), a company can be held liable for data privacy and cybersecurity-related incidents caused by third-party service providers. As a result, the Buyer needs to conduct cyber diligence on these entities. At the outset of the diligence process, the Buyer should request a list of all the Target's service providers and vendors, and any agreements that are above a preset materiality threshold. The focus of this review should be on service providers that have access to the Target's data, such as IT support, outsourced human resources, software developers, data servers and storage providers, and security providers. The review should include not only the service agreement and primary contracts, but also any terms of service, privacy notices and similarly related and relevant documents.

For service providers, the diligence process should aim to identify what obligations and liabilities are created by these relationships and how the Target mitigates these vulnerabilities. Questions that should be considered include the following:

- Are there adequate provisions in the agreements to provide comfort to the Target that its data is sufficiently protected?
- Are there any reciprocal requirements imposed on the Target company?
- Are there indemnification or allocations of liability provisions?
- What types of data are being shared or processed? Are there specific obligations that arise from those types of data (e.g., HIPAA requirements for health data)?
- Are any jurisdictions involved outside that of the Target? If so, do the agreements and procedures adequately satisfy laws and regulations of both jurisdictions? Are there any cross-border transfer issues?
- Do third-party vendors and service providers have their own vendors and service providers?
- Are the contracts consistent with any applicable Target vendor management policies?

The Buyer should also evaluate how the Target selects and monitors these third-party service providers.

The review of customer contracts will focus on any obligations and liabilities in those contracts to which the Target has agreed. The Buyer should evaluate any service agreements, terms of service, privacy notices, and other relevant documents that define the customer relationship. The Buyer should also determine whether the Target has made any representations

relating to cybersecurity and data privacy when establishing the relationship underlying the transaction and whether those representations appear consistent with the Target's practices, based on the remainder of the review.

As part of the Buyer's review, it should also consider the Target company's cyber insurance policies, if such cover exists. Insurance against data breaches and unintentional privacy violations is becoming increasingly common, both as part of a company's umbrella cover as well as specifically and separately for companies in industries where data is an area of focus. The policies may provide some comfort by mitigating any identified risks or, conversely, identify areas of greater risk. In conducting this analysis, the Buyer must also confirm that a change of control will not affect the cover.

If a Target company has numerous contractual obligations, the Buyer may consider inserting representations and warranties into the purchase agreement to provide additional comfort that there will not be undue liability because of these obligations. There are two types of representations and warranties that Buyers can add. The first is a representation stating that the seller has provided the Buyer with all agreements with vendors and third parties during the diligence process. The second goes further to state that the seller has complied with its privacy and data security contractual obligations. Both representations are less common than some of the representations and warranties described previously, but it may be relevant to include them if some of these issues are uncovered during due diligence and cannot be addressed in other ways.

Conducting diligence: other common areas of focus

Depending on the characteristics of the Target and the context of the transaction, there are a variety of other areas that cyber diligence may include, such as compliance with public representations and industry standards, and the security of the company's IT infrastructure.

In addition to complying with laws and regulations relating to data privacy and cybersecurity, a company may also have obligations that stem from its public representations or from industry standards and best practices. In the United States, for example, (as discussed further in Chapter 9) the primary federal watchdog for data privacy and cybersecurity issues is the FTC, which derives its authority from the FTC Act, which in turn prohibits unfair and deceptive commercial practices. While the FTC has broadly interpreted the FTC Act to require companies to provide 'reasonable' protections for sensitive consumer data, its primary enforcement focus is on ensuring that companies comply with prior statements, such as posted privacy policies or advertisements that tout a company's security measures. A Target that is diligent about cybersecurity and data privacy issues will keep track of such statements and advertisements (or lack thereof) and document its compliance with the Act to protect against an FTC complaint or enforcement action. The Buyer should therefore request such records to consider whether they raise any red flags. The Buyer may also request representations and warranties that provide assurances that the company has materially complied with all such statements and advertisements, particularly if its records regarding compliance are not comprehensive.

On a more general level, the Buyer should also request any records or documents that the Target has that can provide insight into its IT infrastructure and technology inventory, such as network diagrams. These records will help the Buyer to analyse its data mapping and identify security vulnerabilities. The Buyer may also want to consider whether the Target company's

security measures align with the needs and complexity of a Target company's IT infrastructure and technology. Once diligence is complete, a Buyer may request representations and warranties to provide assurance that the Target company has adequate (i.e., commercially reasonable) security measures in place.

Addressing red flags

As the diligence process nears its close, the Buyer should consider the red flags that have been identified and determine whether and how they can be mitigated.

Some issues can be addressed by the Target prior to conclusion of the transaction. For these issues, pre-closing conditions or covenants can be used to ensure that the Target addresses these issues. Generally, this will only work for discrete concerns that can be resolved quickly or concerns that may become more complicated once the transaction is concluded. For example, a pending data access request needs to be addressed quickly, as waiting until the transaction closes will only increase the risk of liability. The Buyer can confirm that the Target has addressed these pre-closing conditions and covenants prior to closing either through additional diligence or the use of representations and warranties confirming that the conditions and covenants have been met.

Other issues may be addressed through representations and warranties in the purchase agreement, which can be integrated into existing sections of a purchase agreement (e.g., compliance with laws) or can form their own separate section. Typically, sellers argue that such representations and warranties should be based on a materiality threshold or on the knowledge of the company or certain officers of the company (or both). The seller's materiality threshold will typically be higher than the one used by the Buyer, but it will be determined by considering many of the same factors as a Buyer will consider in setting its own materiality threshold for its diligence process.

There are more general representations and warranties that a Buyer may consider using to mitigate risks. One common representation that a Buyer may request from a seller has to do with the transaction itself – that, to the best of the seller's knowledge, there will be no adverse effects from the transaction, such as a violation of any applicable laws, internal or external policies and procedures, prior statements or other obligations. An obvious example of this would be a provision in a third-party contract that gives a counterparty the right to terminate the relationship in the event of a change in control.

Purchase price adjustments are another mechanism that a Buyer can use to allocate cyber risk. Specifically, if the Target is unwilling to agree to either pre-closing conditions or representations and warranties, the Buyer may instead be able to negotiate an adjustment in price to account for the costs of remediation or the expected cost of uncovered liabilities and obligations.

Another method a Buyer can use to mitigate the cyber risks identified during its due diligence review is to purchase representations and warranties insurance (R&W insurance). R&W insurance can be purchased by either the Buyer or the Target, but Buyer-side policies are generally more common since Targets generally prefer to limit their continued liability. R&W insurance for Buyers also tends to provide broader cover and longer indemnification periods. A Buyer may offer to purchase R&W insurance in return for the Target's agreement to specific representations and warranties. A Buyer should consider how the cost of such insurance will change the value of the transaction. In addition, R&W insurers will often rely

on the Buyer's due diligence when considering whether and how to provide R&W insurance, including cyber insurance. Thus, if a Buyer's cyber diligence uncovers potential liabilities or does not contain adequate bases for its conclusions, an underwriter may insist on exclusions, such as for historic cybersecurity incidents.

Once the Buyer has done all it can during the transaction negotiation to account for the red flags it has identified during its cyber diligence, it should consider how these will inform its plans to integrate the Target. An extended discussion of post-acquisition issues is beyond the scope of this chapter, but common issues that arise include:

- considering how best to incorporate the Target's database and IT assets into the Buyer's existing IT infrastructure;
- retrofitting the Buyer's cybersecurity policies and procedures to account for any unique cybersecurity obligations or vulnerabilities that the Target company has;
- transferring and converting key data into a format that is compatible with the Buyer's systems;
- remediating any identified red flags that were not addressed prior to closing; and
- implementing monitoring protocols to ensure the Target continues to comply with its data privacy and cybersecurity obligations.

In addition, the Buyer should ensure that it takes into account the newly acquired company when it considers the practicality and lawfulness of its future plans (e.g., ensuring that expansion plans adequately account for any effects on the Target's operations).

Conclusion

In the first half of 2018, more than 3.3 billion records were compromised from hundreds of known data breaches.[19] Countless more breaches are likely to have gone unreported or have still not yet been detected.[20] Every company is vulnerable to a data breach, regardless of the strength of its policies and procedures and the sophistication of its IT security infrastructure. As little as five years ago, these risks were not fully understood, and cyber due diligence may have been an afterthought in the due diligence process. Today it is a necessity. This chapter has addressed some of the key issues that a Buyer should consider in the diligence process as well as some of the key red flags, but a full description of cyber due diligence could easily fill a book. Therefore, to adequately conduct this diligence, it is critical that the Buyer use a professional team that understands cybersecurity risks and the specific material issues that Targets in a specific industry are likely to face.

19 Gemalto, Breach Level Index (last visited 4 March 2019), https://breachlevelindex.com/.

20 Breaches often taken years to be detected or reported. For example, a 2013 Yahoo! data breach was not discovered until late in 2016. See Vindu Goel and Nicole Perlroth, 'Yahoo Says 1 Billion User Accounts Were Hacked', *N.Y. Times* (14 Dec 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

Appendix 1

About the Authors

Megan Gordon
Clifford Chance US LLP

Megan Gordon is a partner in Clifford Chance's US regulatory/white collar group focusing on regulatory, data privacy and cybersecurity-related matters and investigations. Megan co-heads Clifford Chance's US cybersecurity and data privacy group and is a leading member of the firm's global tech group. Her work encompasses a broad range of regulatory matters, including in relation to privacy and US data protection laws and regulations. Megan also has experience advising financial institutions and fintech companies on the use of artificial intelligence and big data in various products.

Daniel Silver
Clifford Chance US LLP

Daniel Silver is a partner in Clifford Chance's litigation and dispute resolution group. He previously spent 10 years as a federal prosecutor, serving in several senior leadership positions and as Chief of the National Security and Cybercrime Section within the United States Attorney's Office for the Eastern District of New York. Daniel co-heads the firm's US cybersecurity and data privacy group. He regularly counsels clients on risk mitigation strategies with respect to cybersecurity and data privacy, including incident response, data breach notification, planning and prevention, interface with regulators and law enforcement agencies, and related civil disputes.

Benjamin Berringer
Clifford Chance US LLP

Benjamin Berringer is an associate in Clifford Chance's litigation and dispute resolution group. He represents clients in cross-border investigations and complex commercial litigation, including class actions. In addition to his litigation practice, Benjamin also regularly advises on regulatory matters arising under US privacy and data protection laws, including

risk mitigation strategies, data breach notification, planning and prevention, and data breach response.

Brian Yin
Clifford Chance US LLP

Brian Yin is an associate in Clifford Chance's litigation and dispute resolution group. He represents clients in cybersecurity and data privacy matters as well as cross-border criminal and regulatory investigations. His experience includes advising a diverse array of US clients on their compliance obligations with respect to the General Data Protection Regulation (GDPR) and US state and federal data privacy and cybersecurity requirements. This includes drafting and revising compliance policies and procedures and advising on new product launches. He also advises companies on data privacy and cybersecurity issues in multinational transactions.

Clifford Chance US LLP
31 West 52nd Street
New York, NY 10019-6131
United States
Tel: +1 212 878 8000
Fax: +1 212 878 8375
megan.gordon@cliffordchance.com
daniel.silver@cliffordchance.com
benjamin.berringer@cliffordchance.com
brian.yin@cliffordchance.com
www.cliffordchance.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-223-7