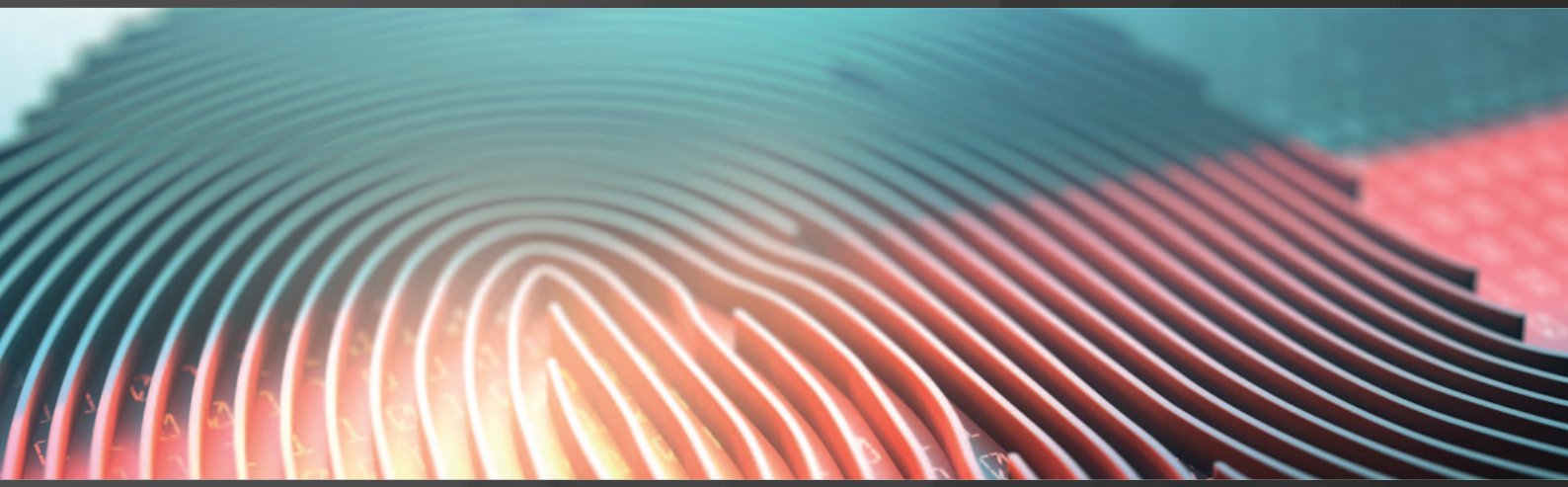
International Comparative Legal Guides



Cybersecurity 2020

A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com

Effective Cyber Diligence – The Importance of Getting it Right


Nigel Parker


Alexandra Rendell

Allen & Overy LLP

Data is a valuable asset. Companies are increasingly seeking to acquire or merge with data-rich targets as a means to grow and enhance their business and keep pace with the fast-evolving digital environment. However, with the exponential growth of data in our connected lives comes the increased range and risk of cyber threats. Companies must carefully consider cyber risks in any M&A activity they may look to undertake so that they can balance both privacy and data security concerns and risks to their businesses, their investors and their customers, but also to safeguard against unintended consequences that may result from pursuing a target without undertaking sufficient due diligence.

Cyber-crime is estimated to cost the UK £27 billion a year, and the average cost to a large organisation of a data security breach is between £1.46 million and £3.14 million. A serious cybersecurity breach can also have a serious effect on a company's share price; for example, AOL, eBay and TalkTalk saw drops of 23.56%, 7.35% and 14.55% in the month after the announcement of a breach, respectively.

Cybersecurity Incidents may also result in wider losses, including:

- regulatory fines;
- business interruption;
- internal costs, including loss of management time and potentially significant costs incurred in remedying the Incident;
- damages in civil actions; and
- reputational damage and a loss of goodwill.

A cybersecurity Incident may also impact the integrity of the data or intellectual property in an organisation (for example, if information is stolen or deleted). Each of these will clearly have some impact, whether short or long term, on the value of a business. Taking measures to mitigate these risks, including undertaking effective cyber diligence, will therefore be of significant interest to any potential purchaser of a business.

What Do We Mean by Cyber Diligence?

Cyber diligence will be most effective when it is tailored to the business and transaction in question, so it essential to consider the scope of any diligence required at the outset. In some cases, high-level enquiry may be sufficient. However, in others, a more detailed examination will be required, and in some cases it may be beneficial to enlist the help of specialist technical experts.

Effective cyber diligence requires considering a number of questions to help scope the risks and the nature of the diligence required.

- **Is it a high-risk target?** Does the target regularly handle data that would make it attractive to a hacker? For example, does it operate in a sector that may increase its risk, such as the medical or healthcare sector, or defence and security? Does the target have a lot of valuable intellectual property that may increase its risk? Does the target operate in a high-risk jurisdiction?
- **Is the purchaser under an obligation to conduct due diligence?** Regulators in certain sectors are starting to request cyber diligence from entities they oversee. For example, the New York State Department of Financial Services enacted a regulation setting out cybersecurity requirements for financial services companies, under which the NYDFS has made clear it expects covered entities to have "a serious due diligence process, and cybersecurity should be a priority when considering any new acquisitions".[1] Any purchaser that is subject to specific regulatory requirements will need to ensure that the level of diligence conducted will meet regulatory expectations, as well as acting to mitigate commercial risks to the company.
- **What sort of data does the target handle?** Does the target regularly handle large amounts or personal data, or sensitive data? Is the target business primarily focused on processing consumer data, rather than business-to-business transactions? If so, it will be particularly important to consider data security and data protection compliance and processes.
- **What effect would loss of data have on the target?** In other words, how valuable is the relevant data to the business?
- **What data security systems and processes does the target have in place?** Cyber diligence should always involve an assessment of technical systems and governance policies and processes around data security, including business continuity and recovery plans. The scope and detail of this assessment will be informed by the cyber risk facing the target.
- **Does the target have a history of cyber attacks and data breaches?** Not all cyber Incidents must be reported under applicable laws, and many will not be. However, the target may keep an internal log of lower-level Incidents that were remedied without the need for any public statement, and so an early review of this (or asking early questions of management) will help inform the scope of further diligence that may be required.

What Might Effective Cyber Diligence Involve?

A cyber diligence process may involve a number of different activities, depending on the cyber risks identified for the target and the scope of the diligence that has been agreed. Each may uncover a variety of technical, legal and financial risks to the target business that a purchaser can consider in its overall assessment of the proposed acquisition. An effective cyber diligence process will also typically involve input from multiple teams, including legal advisors, technical advisors, day-to-day business teams responsible for managing the relevant data, and senior management.

- **Assessment of information assets:** It is essential to understand the nature of the data assets of the target. An assessment of these assets should cover: the value of the assets to the target; how and where they are held (for example, in the cloud, on proprietary servers, etc.); and contractual terms governing those assets, including in relation to transfer and security.
- **Security audits and risk assessments:** As a starting point, the purchaser may wish to use its own risk assessments and security audits as a guide to the principal issues to consider for diligence

© Published and reproduced with kind permission by Global Legal Group Ltd, London

of the target. If the target has a mature cybersecurity policy, it may also be able to provide copies of its own security audits for review. If, however, the target has never conducted its own security audit, or previous security audits have only been conducted by internal teams, the purchaser may wish to consider instructing its own advisors to conduct an audit. Studies have shown that security issues are more typically discovered by external third parties (such as auditors, security vendors or law enforcement agencies) than by internal teams. However, if the target agrees to an independent audit as part of the diligence process, a well-advised target may wish to commission its own report and then share this with the purchaser so as to retain as much control over the process as possible.

- **Regulatory compliance:** Assess the target's compliance with all relevant legal and regulatory standards in the jurisdictions in which it operates. This can involve public searches to confirm appropriate registrations have been made where required, a technical review of the security of the target's information assets, and a review of the policies and procedures that the target has in place to monitor security and report on it where necessary. A policy review should not only capture whether the relevant policies are in place, but also the extent to which those policies are implemented and monitored in practice (for example through internal audits or staff training programmes).
- **Historic breaches and recovery plans:** The purchaser should assess the target's history of data security breaches and how they were addressed. This assessment should cover:
  - the nature of the breaches (for example, whether triggered by internal or external factors);
  - the effect of the breaches on the target (including economic loss, business interruption and wider issues such as reputational damage);
  - how the target responded to those breaches; for example,: how quickly was the breach discovered? Was an Incident response procedure triggered, and if so what level of reporting took place? What remedial measures did the target put in place?; and
  - what, if any, steps did the target take following the breach to prevent reoccurrence?
- **Third party risk:** Consider the target's data sharing practices and arrangements with third parties, particularly if there are any third parties the target relies on to process, hold or otherwise manage its information assets. Review the contracts in place between the target and those third parties and consider how they may affect the target's risk. For example, does the third party have clear reporting obligations in the event of an Incident? Does the target have appropriate contractual protection (such as indemnities) if the third party breaches its obligations? The purchaser should also enquire as to what diligence the target did on the third party before, or during, the contractual relationship – has the target conducted any security audits on the third party to check how the third party protects information assets?
- **Employee risk:** Consider the target's internal policies and processes and how the target ensures that employees and senior management understand the cybersecurity risks facing the business and how to mitigate them. This may include an assessment of the target's internal governance structure for cybersecurity matters to understand who has day-to-day oversight of compliance. It will also typically include a review of the target's internal education and training programmes, internal compliance assessments and the nature and extent of cybersecurity information reported to the board.

Considering these issues as part of an effective cyber diligence process will not only help provide a more detailed insight into the target's network and technology risk profile before a merger or acquisition, but can also be used post-acquisition to help shape integration planning.

Case Study – Yahoo

In December 2014, Yahoo (now known as Altaba) suffered a massive breach of its user database resulting in the theft of hundreds of millions of its users' data. Yahoo discovered the breach within days, and Yahoo's Chief Information Security Officer notified the senior management and legal teams. However, Yahoo did not publicly disclose the breach until 2016 – in connection with an acquisition by Verizon Communications. In the intervening period, Yahoo had both failed to disclose the breach in its risk factor disclosures in annual and quarterly reports and in the due diligence process with Verizon. In total, all of Yahoo's three billion users were likely to be compromised.

The SEC found that Yahoo violated various provisions of the US Securities Act and the US Exchange Act in respect of market disclosures and misleading investors, and imposed a fine of $35 million – the SEC's first ever against a public company for failure to disclose a cyber breach.[2]

The other key consequence for Yahoo was the impact on the Verizon deal. Prior to the disclosure of the data breaches the parties agreed a purchase price of $4.8 billion. Following the disclosures, completion of the deal was delayed while the parties worked through the impact, eventually agreeing a revised price of $4.48 billion – a discount of $350 million. In addition, the two companies agreed to share legal and regulatory liabilities. While $350 million may seem like a heavy price to pay for Yahoo, it was rumoured at the time that Verizon was looking for a discount of $1 billion on the agreed purchase price.

Case Study – Marriott

A more recent example of unintended consequences following an M&A transaction, which again helps to highlight the importance of cybersecurity due diligence, is the UK Information Commissioner's (**ICO**) recent announcement of an intention to fine Marriott International, Inc. over £99 million for GDPR infringements following a data breach that was notified to the ICO in November 2018.

A variety of personal data contained in approximately 339 million guest records globally were exposed by the Incident, including some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (**SPG**) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiry dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). Around 30 million guest records related to residents of 31 countries in the European Economic Area (**EEA**), and 7 million related to UK residents.

The Incident related to systems of the Starwood hotels group, and in particular the Starwood guest reservation database, which are believed to have been compromised in 2014. Marriott subsequently acquired Starwood in 2016 in a $13.3 billion takeover.

At the time of writing, the ICO has only published its intention to impose a fine, and so the ICO's public statements on the matter are comparatively brief. The ICO will consider any further representations by Marriott and will not publish any final enforcement notice, which would contain further detail of the relevant breaches and the basis for the ICO's decision to impose a fine, until the ICO has made its final decision. However, it is worth noting that in the ICO's statement,[3] the ICO drew particular attention to purported due diligence failings by Marriott in relation to the 2016 Starwood acquisition, saying "[t]he ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems". It remains to be seen what further conclusions the ICO will draw as to the impact a lack of sufficient cybersecurity due diligence had in this case.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Endnotes

1. https://www.dfs.ny.gov/industry_guidance/cyber_faqs.
2. https://www.sec.gov/litigation/admin/2018/33-10485.pdf.
3. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Alexandra Rendell is a senior associate specialising in commercial contracts, data protection, intellectual property and information technology law. Alexandra advises on complex commercial arrangements for a range of clients in the technology, life sciences and financial services sector, including outsourcing and service provision arrangements, licensing and IP/data exploitation.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 2639
Email: alexandra.rendell@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, anti-trust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

© Published and reproduced with kind permission by Global Legal Group Ltd, London