Cybersecurity: considerations for M&A practitioners

William Samengo-Turner and Nigel Parker
Allen & Overy

global.practicallaw.com/w-014-3753

THE NATURE OF THE CYBERSECURITY THREAT
As our lives become increasingly connected and businesses move more of their assets, systems and operations online, the range of cyber threats increases. The UK Government has classified the threat posed by breaches of cyber security as "Tier 1" and, in the context of a commercial enterprise, it is easy to see why; cyber-crime is estimated to cost the UK 3.6% of 2020 GDP. The average cost to a large organisation of a data security breach is between £22.5m and £28m million. The effect of a serious cyber security breach on a company's share price can be significant (in high profile examples, AOL, eBay and TalkTalk saw drops of 23.56%, 7.35% and 14.55% in the month after the breach, respectively).

A cyber incident may result in a wide range of losses, including:

- Economic losses, including interruption to business.
- Internal costs (for example, the time involved in identifying, remedying and managing the fall-out incident).
- Out-of-pocket expenses (such as legal advice and forensic investigators).
- Regulatory fines.
- Damages awarded in civil actions.
- Damage to market reputation and goodwill.

An incident may also result in the theft or deletion of information and intellectual property (IP) or may see criminals tamper with the integrity of an organisation's data.

In addition to the attacks that hit the headlines, there are hundreds of thousands of lower-level attacks, which are arguably more of concern to organisations from a risk management perspective, as little or no technical expertise is necessary. Malicious software can be downloaded from the internet for free by almost anyone and then used to launch an attack and wreak havoc on a business' IT infrastructure.

Clearly, any such risk is of significant interest to a potential purchaser of a business. In this article, we will consider how best to assess these risks and the possible steps to mitigate these issues if discovered.

DIFFICULTIES WITH THE PRESENT LEGAL FRAMEWORK
One of the issues for advisers assessing a target's cybersecurity is that the laws governing the risk associated with cybersecurity are dispersed and given at a high level. In particular, there is not a single set of mandatory cybersecurity controls or rules with which companies must comply. Instead, there are a number of different laws, rules and regulations which may apply depending on the context of the relevant incident and the nature of the organisation involved.

While recent legislative changes (notably the introduction of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR))) have brought greater certainty to the regulatory environment, there are a number of important areas in which companies are left to largely self-regulate. Matters such as employee and director training, reporting obligations and audit requirements are interpreted by companies in a number of different ways.

In the context of M&A transactions, the relatively uncertain regulatory landscape therefore means that practitioners do not have a clear set of rules against which to assess potential targets and must give careful thought as to how best assess a target's cyber risk during due diligence.

DUE DILIGENCE: WHAT IS EFFECTIVE CYBER DILIGENCE?
Identifying the risk environment

Given the constantly evolving nature and variety of cyber-attacks, it is important to tailor any diligence to the target at an early stage. Different businesses will be subject to differing vulnerabilities and threats, and, while some transactions may only require a high-level enquiry, others may call for a thorough examination and, in certain cases, the involvement of forensic or technical experts. To assist in scoping the cyber diligence, the following questions should be considered:

- **Does the deal relate to a high-risk target?** A business' cyber-risk can be increased by a number of factors. Companies which handle a large amount of sensitive or personal data (such as financial services firms or medical care providers) will be attractive to hackers. Similarly, those which generate or own valuable IP (such as aerospace or tech companies) have a raised level of risk. Geopolitical factors should also be considered, particularly where state operators may wish to obtain a company's confidential information (defence and security being a particularly vulnerable sector).

- **What is the nature of the data being handled or held by the target?** If a large amount of personal or sensitive data is being held, it will be particularly important to consider the target's data protection compliance and processes. As part of this review, it is important to assess how valuable the relevant data is to the business (and what affect any loss or breach in respect of this data would have on the business and on individuals).

- **What is the nature of the target's data protection systems and processes?** Regardless of the level of cyber risk faced by the target, a proper assessment of its technical systems and governance processes (including recovery and business continuity plans) should be made. Where there is an increased cyber risk, the scope of the diligence in these areas should also be increased and a forensic review by specialist IT experts may be considered.

- **What is the target's history of cyber attacks and data breaches?** While public searches may give an indication of significant historical problems, they are less likely to reveal...
lower-level problems or issues which were remedied without the need for a public statement. An early review of the target’s data breach or incident management log (if available) and interviews with management will assist with diligence scoping in this regard.

**Performing cyber diligence**

Once the cyber risk has been ascertained and the diligence process scoped accordingly, there are a number of cyber-specific diligence practices to consider. Each diligence exercise will be different and not all of the following matters will be relevant for every target. Some examples of these due diligence exercises include:

- **Information assets.** A comprehensive understanding of the data assets held by the target is an essential first step in any cyber diligence. The purchaser should appraise itself of the nature of these assets, their value to the target business, the manner in which they are held, and, if the assets are held on the cloud or otherwise remotely, the contractual terms on which they are held, transferred and protected.

- **Risk assessments and security audits.** The highly technical nature of the systems and processes needed to maintain a firm’s digital security means that the purchaser’s traditional professional advisers may not have the requisite technical expertise to fully appraise the target. However, the company’s risk assessments and security audits should provide an overview of the principal issues and help orient further diligence, if required.

If the target has a mature and well-developed cybersecurity policy, it should be able to provide the prospective purchaser with copies of its periodic security audits. Ideally, these audits will, at least on occasion, have been performed by independent third parties not least because studies have shown that security issues are more typically discovered by external third parties (such as an auditor, security vendor or law enforcement agency) than by internal teams.

If an established company has never conducted a third-party audit, the purchaser may wish to consider instructing its own advisers to perform a review of the target’s systems and networks. This review may even include searches of the dark web (that is, an area of the internet which can only be accessed using specialist tools and in which hackers and other cyber criminals often trade assets) to see if any of the target’s information assets are available there. If agreeing to such an audit, a well-advised seller should opt to commission its own report and provide it to the purchaser so as to maintain as much control over the sales process as possible.

- **Regulatory compliance.** Enquiries should be made to ensure that the target meets all of the relevant regulatory standards and practices in the jurisdictions in which it operates. This will not only relate to the security of the company’s information assets, but also to the processes it has in place to monitor security and report on it when necessary.

- **Breach experience and recovery plans.** An assessment of historic breaches of data security suffered by the target should be made. These enquiries should consider:
  - the effect of those breaches on the company (these could extend beyond the immediate loss of data to include both financial and reputational loss);
  - the target’s immediate response to those breaches (including time taken to discover the breach, level of reporting and remedial measures); and
  - what, if any, steps were taken following the breach to ensure that similar attacks are prevented.

- **Third-party risk.** If the target’s business relies on third parties to process, hold, transfer or otherwise manage information assets, it is important to review the contracts under which these arrangements are governed. Points to consider include:
  - how does the third party protect and store the data?
  - what are the third party’s data protection measures?
  - what protection (indemnities) does the target have if the third party breaches its obligations?; and
  - what are the third party’s reporting obligations and how often does the target audit or check the security of its processes?

- **Employee risk.** A well-advised buyer will wish to assess the target’s internal processes to ensure that employees and senior management understand the business’s cybersecurity risks and policies. This will typically include:
  - a review of the target’s education and training programmes;
  - an assessment of the nature and extent of information reported to the board; and
  - an understanding of who in the company has day-to-day oversight and responsibility of the target’s cybersecurity.

For companies with increased cyber risk, it is important to assess how knowledgeable the employees and management are of these risks and the steps taken to mitigate them.

**DUE DILIGENCE: WHAT RISKS MIGHT BE DISCOVERED AND HOW CAN THEY BE ADDRESSED?**

An effective cyber diligence process may uncover a number of technical, financial and legal risks in the target business. As with any diligence discovery, the nature and extent of these risks may affect the final terms of the deal, the level of consideration or, if very serious, the viability of the deal itself.

Possible threats may include:

- An ongoing breach or attack.
- An unrevealed previous breach.
- A persistent intruder or vulnerability to its systems.
- A dirty, malware-ridden environment.
- Inadequate security measures and corporate governance processes.

For detailed descriptions of the threats, see box, *Risks that may affect the final terms of the deal*. 

---

[global.practicallaw.com/acquisitions-guide](http://global.practicallaw.com/acquisitions-guide)
Risks that may affect the final terms of the deal

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ongoing breach or attack</td>
<td>A malicious third party currently controls or has access to part or all of the target systems.</td>
</tr>
<tr>
<td>Unrevealed previous breach</td>
<td>The target has suffered a past breach about which it was unaware but which is no longer a material issue to the business.</td>
</tr>
<tr>
<td>Persistent intruder/systems vulnerability</td>
<td>The target systems host an attacker or virus which would allow a third party to gain access at a future date.</td>
</tr>
<tr>
<td>Dirty environment</td>
<td>The target systems do not contain any critical threats or issues but do have a considerable amount of common malware.</td>
</tr>
<tr>
<td>Inadequate security measures and corporate governance processes</td>
<td>The target company’s internal governance processes and systems are inadequate and pose a risk to ongoing security compliance, detection and reporting.</td>
</tr>
</tbody>
</table>

Response to diligence and contractual terms

Assuming that the risks identified in diligence are not so significant as to make the deal unviable, it may be necessary to consider the inclusion of specific deal terms in response to the discovered issues. These can be broken down into four principal areas:

- Warranties.
- Specific indemnities.
- Closing conditions.
- Pre-closing covenants.

Warranties

Where data security is identified as a particular risk or concern, the warranty package should be amended to reflect this focus. Special attention should be paid to the following areas (some of which may overlap with other, more general warranties):

- **No security incidents.** This is a warranty that the target has not suffered any cybersecurity incidents within a certain period prior to the date of the agreement. The definition of “incident” will be the subject of negotiation but could include hacking, electronic theft, phishing, spoofing, pharming, “man-in-the-middle” attacks, denial of service attacks, malware infections or other threats to the company’s cybersecurity.

- **Downtime.** This is a warranty that the target has not suffered more than a certain number of incidents of systems downtimes (for example, that it has suffered no more than two incidents lasting for four-hour periods during the two years prior to the date of the agreement).

- **Third party data-sharing agreements.** Warranties should be included in respect of any arrangement by which data is shared, managed, retained or otherwise handled by a third party.

- **Compliance with laws.** These warranties should consider both compliance with laws and regulations (with specific reference to applicable data security legislation in the relevant jurisdiction included) and the target’s data security policies. The seller should also warrant that it is not subject to any regulatory investigations nor is it reasonably likely to be so.

When considering provisions limiting the seller’s liability in respect of warranty claims, it may be appropriate to consider separate caps in respect of claims which arise out of the cybersecurity warranties. If a post-completion security audit is proposed, care should be taken to ensure that the time period in which the purchaser may make a claim expires after the completion of that audit so as to allow enough time to make a claim.

Data breaches often give rise to third-party claims. Customers and clients of the business which has suffered the breach may seek compensation or require careful management. It is therefore important to consider the provisions of the agreement governing the conduct of such claims. The purchaser, as the owner of the business, will want as much control as possible. Equally, the seller, if it is to underwrite some or all of the costs, will want increased oversight and an ability to restrict the purchaser from entering into gratuitous settlement arrangements.

**Specific indemnities**

As with more traditional risks, if particular problems are discovered which need to be remedied, a specific indemnity may be appropriate. The terms of the indemnity (and, in particular, any caps) will depend on the nature of the issue. However, the drafting may be complicated by the fact that, in the context of cybersecurity, potential liability is often difficult to quantify.

Where a seller is reluctant to agree to an open-ended indemnity, a cost-sharing arrangement may be an alternative approach. This could, for example, be structured as an indemnity in respect of remediation costs (which will be easier to quantify) together with an agreement to share costs in respect of claims from customers or other third parties who have suffered as a result of the breach.

A well-advised seller will be likely to seek a limitation on the period during which the purchaser can make claims under the indemnity. Given that the resolution of cybersecurity issues can often be slow and involve a long list of claimants, it will often be reasonable for a purchaser to insist on a relatively long claim period.

As with warranty claims, careful thought should be given to provisions governing the conduct of third-party claims.

Closing conditions

Where remediation activity is necessary, a decision will need to be made as to whether the remedy should be effected either:

- Prior to closing (typically at the expense of the seller).
- After the deal has closed (at the expense of the purchaser, but potentially the subject of an indemnity or cost sharing arrangement [see above, Specific indemnities]).

The chosen approach is likely to be influenced by the severity of the risk and the purchaser’s appetite to bear the risk of issues arising during the remediation process. The inclusion of a completion condition allows the purchaser to walk away from the deal if the problem is not fixed and therefore provides the best protection for the purchaser.

Typically, the seller will seek to resist all but essential conditions. Remediation of an existing security issue or ongoing breach is likely to fall into this category. Other areas which may be the subject of negotiation include: 
• The implementation of new IT safeguards or systems.
• Addressing compliance gaps.
• Amending contracts which relate to the handling of data by third parties.

**Pre-closing covenants**
The purchaser should consider including specific provisions in relation to cybersecurity and the handling of data prior to completion. These could relate to:

- The sharing or handling of data during that period (particularly where the purchaser has determined issues in this area through diligence).
- Ongoing security arrangements prior to completion.
- The conduct of investigations prior to completion.

The purchaser may also seek a right to be consulted on, or participate in, any remedial actions to be taken by the seller or discussions with regulators.

**BUSINESS SALES AND OTHER CARVE-OUTS**

**General issues**
Business sales and carve-outs raise their own particular issues from a data security perspective. In particular, data migration can be complicated due to one or more of the following factors:

- **Costs.** Properly segregating data is costly and time consuming, and often requires considerable manpower and planning. If compromises are made in the interests of reducing costs, the risks of data being treated improperly or lost are increased.

- **Technical constraints.** The challenges posed by data transfers are considerable and can lead to information assets ending up in the wrong hands with inadequate controls. Therefore, appropriate “wrong-pockets” clauses and agreements as to the treatment and protection of data should be included in the transaction documents.

- **Ongoing agreements.** If data is either shared or maintained for a period of time post-completion, appropriate transitional agreements will be required (see below, *Transitional service agreements*). However, such arrangements raise information security risks and should be avoided as a long-term solution.

**Transitional service agreements**
Many transactions will require transitional service agreements to allow for the ongoing support of the target by the seller’s group for a period after completion. The activity of IT functions (which are often centralised by businesses) is a common service under these agreements. Therefore, it is important to ensure that the appropriate controls (particularly with regard to data) are put in place. Such controls could relate to, for example:

- **Technical and organisational access controls.** The recipient of the service will want to ensure that its technical specialists have proper access to the relevant systems insofar as they service the target business. This can cause complications in relation to confidentiality and system security, and must therefore be structured carefully.

- **Auditing and monitoring.** The recipient of the services may wish to ensure that it has a right to audit and/or monitor the service provider’s systems and practices.

- **Ensuring compliance with purchaser policies.** The purchaser may want to require that any services are provided in accordance with its own information security policies (or those of third parties which it has agreed to follow), particularly where diligence has demonstrated that the target and/or its parent group have historic cyber issues. Agreeing to provide the services on these terms may be costly, difficult or even impossible for the seller.

**CYBER INSURANCE**
Where diligence has uncovered risks but the parties are unable to agree an appropriate contractual remedy, it may be appropriate to consider specific cyber insurance. Like warranty and indemnity insurance, the level of cover (and the cost of any premium) is influenced by the thoroughness and quality of the due diligence exercise performed. Accordingly, if cyber insurance is contemplated as part of the deal, consideration should be given as to when and how the due diligence should be shared with underwriters and the impact on the deal timeline in negotiating the policy.

**INTEGRATION PLANNING**
A common cause of IT vulnerability for organisations is the presence of overly complex or conflicting systems borne out of a failure to integrate following an acquisition. As a company acquires other businesses, the acquired entities’ systems are either partially connected to the parent’s network or operate independently. Increased complexity of this nature will often lead to an increased risk of weaknesses which can be targeted by hackers or other criminals.

It is for this reason that acquirers are increasingly considering the challenges of integration as early as possible in the transaction and, in particular, during the due diligence process. Consideration should be given in relation to whether specific questions should be asked during diligence, in order to give the acquirer’s IT team the information it needs to develop an integration plan, as early as possible. Alternatively, it may be appropriate for the transaction documents to include specific covenants to ensure that appropriate co-operation will be given to the party’s respective IT teams, between signing and completion, to help plan an integration strategy.
William Samengo-Turner, Senior Associate

Allen & Overy
T +44 203 088 4415
E William.Samengo-Turner@AllenOvery.com
W www.allenovery.com

Professional qualifications. England and Wales, Solicitor, 2009

Areas of practice. Corporate/M&A.

Non-professional qualifications. MA (Oxon), Modern History, University of Oxford, 2005; Graduate Diploma in Law, Oxford Brookes University, 2006; Legal Practice Course, College of Law Moorgate, 2007

Recent transactions

• Advises some of the world’s leaders in technology on a range of issues including M&A, joint ventures, board advisory, corporate finance and cybersecurity.

• Has spent considerable time living and working in Silicon Valley as a secondee to the offices of Fenwick & West, one of America’s leading life sciences and technology firms.

• Advised entities in the tech sector and its related industries both in Europe and the US, from emerging enterprises and start-ups to large public corporations.

Nigel Parker, Partner

Allen & Overy
T +44 203 088 3136
E Nigel.Parker@allenovery.com
W www.allenovery.com

Professional qualifications. England and Wales, Solicitor, 2005

Areas of practice. Corporate/Commercial and Data protection, specialising in intellectual property, data protection and privacy, commercial contracts and IT law.


Recent transactions. Advised clients on strategies for managing legal risk in relation to cyber-security, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking positive action in response to attacks.

Professional associations/memberships. International Association of Privacy Professionals (IAPP).