*Thank you for attending the '**M&A – Cybersecurity and data privacy risks**' webinar by CRMG and Collyer Bristow. Below are questions from the audience that were unable to be answered due to time running out. CRMG and Collyer Bristow have provided detailed answers. Please note that the answers given represent the individual views of both organisations who have significant experience in cyber risk and/or legal matters.*

*We hope this is helpful, and for any further questions please contact us at **info@crmg-consult.com** or **info@collyerbristow.com**.*

- **To Simon's threat question, how do you validate the cyber risk assessments done at the firm being acquired?**

  To validate the cyber risk assessments, we would suggest ensuring that:
  1. a leading methodology has been followed
  2. the scope of the risk assessment covers the essential aspects of the firm being acquired or the entire firm
  3. the risks that have been identified have been mitigated (i.e. controls have been implemented or there is a plan to implement).

- **Question for Howard, is there a strict cyber due diligence framework that is covered in Collyer Bristow's standard due diligence process?**

  The scope of the due diligence and the questions we would ask of the Seller will very much depend on the nature and size of the target business. However, we would almost invariably cover the following areas:
  - *capital structure (assuming a share purchase);*
  - *accounts and management accounts;*
  - *assets;*
  - *debt and other liabilities;*
  - *commercial contracts (customers, suppliers, distributors, etc);*
  - *employees;*
  - *intellectual property;*
  - *IT, data protection and cybersecurity;*
  - *real estate;*
  - *litigation and disputes.*

  Other areas might be relevant, depending on the target business's activities. For example, we would ask more environmental questions if the business carries on any manufacturing; the scope of the Bribery Act questions might change depending on where they do business and the extent to which they use external agents for that; we might want to consider competition/anti-trust rules if the parties have a significant share of the relevant market; and we'll ask about licences and consents, if it's a regulated business etc.

Continued…

- **Do you expect all this information to be shared before the contract is signed? If not isn't it too late after the sign-off?**

  From an information security perspective – Yes. If you are acquiring technology, IP, a product, knowing how they have protected this asset from cybersecurity threats (e.g. Nation states copying the IP) is vital. If the organisation has experienced a cyber attack/data breach but did not disclose this, then the acquiring company is effectively taking on that risk without knowing.

- **What you've described looks pretty advanced to me. Would you really expect to see everything Simon has described?**

  Cybersecurity and cyber risk are a growing concern for all organisations. We are ALL seeing impacts on organisations that leads to irrecoverable reputational damage in many cases and this will continue to grow. Organisations are taking this seriously and an approach to assessing cyber risk has to be conducted in a rigorous manner to identify the risks and also to assure regulators that the risk assessment has been conducted.

- **Would a lawyer really be expected to handle all this as part of a due diligence process themselves?**

  The purchaser's solicitors are always involved in drafting the questionnaire and the vendors solicitors involved in preparing the responses. How much involvement they respectively have in the DD process itself varies from deal to deal and depends partly on the extent to which the clients are willing to incur fees for the solicitors' work in the process. Certainly, the solicitors cannot be part of the process without their clients' involvement.

  The solicitors will review the information provided by the Seller and produce a report for the Buyer setting out their findings. The Buyer should take account of these findings in negotiation of the purchase agreement.

  Depending on the nature and size of the target business, other specialist advisors may be involved, to enquire more deeply into key areas.

- **What can/should buyers do if they discover a problem during due diligence?**

  Depending on what the Buyer has discovered, the Buyer might do any (or a combination) of these:
  - Ask the Seller for more information, so he can properly assess the implications of the problem;
  - Require the Seller to put the problem right before the Buyer proceeds any further;
  - Require the Seller to give further warranties and/or indemnities in relation to the issue;
  - Adjust the purchase price to take account of any remedial action needed;
  - Withdraw from the acquisition entirely.

  As a reminder, a warranty is a commitment by the Seller that a given fact is true. If the fact proves to be false, the Buyer is entitled to compensation. This compensation is based on the reduction in value of what the Buyer has acquired – what are the shares worth, as against what they would have been worth had the statement been true. It's important to see from this that the compensation is

not a simple adjustment to reflect the cost to the Buyer of dealing with the problem. In practice, the compensation can often be significantly less than the true cost.

On the other hand, an indemnity is a promise by the Seller to pay to the Buyer the pound-for-pound cost of the matter indemnified. For example, if the Buyer is worried that they will have to pay compensation, or a fine, because of a data breach, they can require the Seller to give an indemnity in respect of that compensation/fine.

It might seem from this that a Buyer would want many indemnities. However, market practice is that indemnities are fairly rare (other than in relation to tax matters) and generally relate only to very specific concerns discovered in due diligence. So a Buyer shouldn't go into a process thinking that they will be able to get broad indemnities and using that as an excuse not to do their own due diligence investigations properly.

From the Seller's perspective, this is why it's important to review carefully the information you put in the data room in advance. That way, you can do any remediation in advance of the Buyer raising the problem with you, or at least be prepared for how you're going to respond to the Buyer's pushback in negotiations.

- **What can/should buyers do if they discover a problem after they've completed the acquisition?**

The Buyer should look carefully at the terms of the warranties and indemnities given by the Seller, to see if the problem is covered by any of those. If it is (or might be) then the Buyer should look at the requirements in the agreement for making any claim. For example, there will almost always be strict time limits and procedural steps which must be followed accurately; otherwise the claim risks being invalid. There are likely to be other limitations, including in particular (for warranty claims) an obligation on the Buyer to take steps to mitigate (minimise) his loss.

We therefore strongly recommend that the Buyer seek legal advice urgently upon discovering a problem with what he has acquired.

Disclaimer

The information and opinions contained here are for general interest and information purposes only and are not intended to constitute specific legal, commercial or other professional advice and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances, While we seek to ensure that the contents are not misleading or outdated, users should obtain specific legal advice before making or refraining from making any business or personal decisions.