CYBER SECURITY DUE DILIGENCE IN M&A TRANSACTIONS

Robert Bond, Partner, Bristows LLP, London

1 INTRODUCTION

This paper will focus on the steps that every business should have taken to test and evaluate the cyber security policy of a business which it is considering to acquire. It will also provide the target business with pointers as to what it needs to do to present its data and cyber assets in the best light.

It goes without saying that every company should have a cyber security policy that addresses prevention rather than cure but it is clear whatever preventative measures are put in place there is likely to be an incident and without a plan as to how to respond to the incident then what is at the time a crisis will likely become a disaster. It is not sufficient for a business to have a plan; it is important that the plan must have been promulgated, distributed, tested and revised on a regular basis.

The effect of a cyber incident has a direct impact on the value of the business; a business with a good track record and robust procedures and processes will, in general, secure a higher value than a business with a poor record and inadequate processes. It is therefore of prime importance to both seller and buyer to ascertain precisely what the cyber issues are through a robust due diligence process.

2 PREPARATION

In order to determine the preparedness of a business for a cyber incident we must first understand what the risk profile looks like! The range of incidents is large – from inadvertent disclosure of business secrets via email, the disclosure of confidential information via social media, the failure to protect data and information in physical form, the inappropriate use of insecure communication and hosting tools and services, the failure to identify cyber-criminal attacks through social engineering and emails, the breach of security by employees, contractors and disgruntled former employees and hacking in a variety of forms and by a variety of players. The list goes on and on. Businesses need to have prepared policies and procedures to enable their staff to recognise them and implement technical and organisational measures to repel and/or prevent such incidents.

When an incident is identified there needs to be a "rapid reaction taskforce" in place to ensure that further loss is minimised. The make-up and experience of such a taskforce is something that a due diligence process should be seeking to establish.

3 RESILIENCE IS A MIND-SET

Businesses are facing an increased compliance requirement as a result of the wide variety of laws and regulations and an inability to address cyber security can lead to a range of breaches, investigations and fines.

It is therefore essential for a business to have in place a policy and procedure to carry out regular assessments or audits of resilience against cyber threats and vulnerabilities.

Due diligence focus should be on the robustness of resilience assessment practices. Attention should be paid to the details of internal and/or external assessments and audits of both organisational measures as well as technical measures.

Resilience cannot be achieved by a "tick box" approach but requires cyber security by default to be in the mind-set of management and staff.

In relation to personal data there is an increasing use of Privacy Impact Assessments (PIA) as a mechanism or tool to ensure that privacy and the security of personal data is embedded in the ethos of the company and the mind-set of employees.

A buyer would not seek to acquire a manufacturing business without a full environmental assessment; where the assets of a business are, increasingly, data, it would be foolhardy to acquire a data rich business without assessing the value of that asset.

4 TRAINING AND EDUCATION

Policies and procedures are of little value if they are not appropriately communicated throughout the business and without training and education individuals in the business may not fully understand their duties and responsibilities or the consequences of their failure to follow policies and procedures.

Due diligence should be taken to ensure that the company has in place technical and organisational measures to show that policies and procedures have not only been distributed throughout the business but that the individuals that have received the policies have read them, understood them, been trained on them and have signified an intention to adhere to them.

There are third party products and services available to assist in the roll out of policies and procedures as well as training solutions, so due diligence should be taken to see what products are being used and also to understand any roles and responsibilities as well as risks and liabilities in the use of those third party products.

5 DATA MANAGEMENT, THIRD-PARTY RISK, EMPLOYEES AND OTHERS,

It is never too early in the acquisition process to commence the due diligence exercise in relation to cyber security as it is unlikely that the target company will have all the information immediately to hand and depending on the outcome of the enquiries, the direction and price of the transaction may be affected.

From the target's perspective, the information which is to be provided is particularly price sensitive and may not have been made public previously – either to customers, suppliers or regulators. A detailed non-disclosure agreement should be put in place before any information is provided. This may encompass personnel in both target and acquirer who are not involved in the mainstream part of the deal.

5.1 Data Management

Before an evaluation can be carried out of the data management risk, it would be necessary to determine precisely what data and other information a target holds; from where the data is acquired (or created if internal); where is it held physically (or virtually); how important is the data to the business; why is it held; what use is made of it.

Experience shows that many businesses themselves do not have full knowledge of the information that they hold – either in extent or in location – or any restrictions which may be placed on the use of that information.

Changing regulatory requirements both domestic and international – and in certain cases, sectoral – mean that the provenance of information is of critical importance to the value of a business. If an acquirer cannot be 100% sure of what restrictions may exist in relation to the assets that it is acquiring, a discount will need to be applied to take account of the risk.

5.2 Third Party Risk

Whilst all contracts with third parties (contractors, suppliers, developers etc.) will need to be evaluated from a due diligence perspective generally, in the context of this paper, what is important is that such contracts (and perhaps less formal arrangements) are investigated to determine whether any third party has any degree of access or interface to the target's systems / data. Where the target has outsourced any part of its administration infrastructure, particular regard will require to be had to those relationships. In practical terms, the third party will need to be treated as if it were part of the target with the same degree of attention applied to its security processes and procedures.

Many cyber breach incidents are the result of the action or failure of a third party contractor. Any incident detection, response and recovery due diligence should therefore consider the position of such suppliers as well as the target.

5.3 Employees

The human factor is just as important as any technical measure; for that reason, particular regard should be had to the target's policies and behaviour towards its workforce. Phishing, or targeted e-mails and lax internal controls can provide just as great a threat to a business as external hacking. Remember to include temporary workers, contractors, consultants and C-Suite executives in the evaluation.

5.4 History

Has the target faced a data breach (of which it is aware) in the past? Once a business has discovered the data breach, (or believes it has suffered one) how it responds is of primary importance. In many jurisdictions there are specific breach notification requirements in relation to a data breach. Did the target comply with such obligations, or did they adopt an ostrich-like approach and hope that nothing bad happened or will happen? If there has been an unauthorised access to the systems and apparent data exfiltration, it should not be assumed that only a small portion of the data set is at risk.

For the acquirer, it is imperative to be aware whether it is purchasing future troubles from affected consumers / businesses / regulators and possibly stockholders as this will condition warranties, price adjustment, or deal terms.

Do not ignore reputational damage, which can be significantly greater than the direct financial loss of an incident.

Assuming that the business is aware of a previous data breach, is there any indication of from where the breach originated; what was being sought – financial, IP, other? An assessment needs then to be made of how the target dealt with the breach and whether it put any steps in place to guard against a repeat intrusion. How the target has approached these issues will be a good indication of any other, presently hidden but lurking issues

6 WHAT POLICIES ARE IN PLACE, WHEN, HOW HAVE THESE BEEN COMMUNICATED, AND HAVE THEY BEEN TESTED?

6.1 What?

Incident Response and Recovery Policies and Procedures are not stand-alone but part of a suite of Policies and Procedures which should be in place across the business. It is not sufficient merely to have these available on the business's intranet or available from

HR; if they are to have any value, they must be living documents that are understood by all relevant employees in the business.

Perhaps they should also interface to the business's ethical reporting policies, after all the effect of the incident may be seen first by someone other than the C-Suite executives or the IT department and, in all cases, time is of the essence.

What therefore are the types of process that should be evaluated as part of the due diligence process[1]?

6.1.1 Policies controlling use by employees, contractors and others of electronic systems, both within the target company's premises and remotely;

6.1.2 Clear reporting lines – both within and outwith the normal whistleblowing processes

6.1.3 Policies in relation to the use of social media by employees and contractors;

6.1.4 Employment / services contracts which include provisions relating to confidentiality, secrecy and Intellectual Property Rights;

6.1.5 IT and systems control and access policies;

6.1.6 System logging policies – what is logged? When is it logged? Does anyone check the logs?

6.1.7 Is there a complete list of all parties with access to the systems, internally or externally, and their level of access?

6.1.8 Who manages the target company's firewalls and similar?

6.1.9 Does the company adopt a policy of installation, after due verification, of all security patches from all its vendors as soon as is possible?

6.1.10 Is there a Policy for BYOD? Can the business remotely wipe mobile / external devices?

6.1.11 Is data encryption used routinely and automatically? Special attention needs to be given to personnel who may be taking company devices internationally? Is there a policy to deal with devices on their return before they are allowed to join the corporate network?

---

[1] This is not an exhaustive list; each target will have its own peculiarities and the scope of the enquiries will be a work-in-progress until Closing or Completion of the deal.

6.1.12 Is there a written process setting out what needs to be done if there is an apparent cyber incident, whether intrusion, ex-filtration or data loss?

6.2 When?

6.2.1 When are Policies communicated to employees / contractors?

6.2.2 When were Policies last updated?

6.2.3 When a Policy changes when are the changes notified to users etc.?

6.2.4 Is there a regular review process involving C level staff?

6.2.5 Is there a record of communication / updates?

6.3 How?

6.3.1 How are the policies communicated to each of the affected groups?

6.3.2 Is there a record of who has opened / read / understood the communications;

6.3.3 Are there any follow up checks made – when / how / to what effect?

6.4 Verification?

6.4.1 Does the affected business engage any external consultant(s) to check its security policies; these should be more than "penetration tests", but should look at the internal security of the business IT infrastructure.

6.4.2 Does the business conduct realistic tests of its response to a cyber incident? This should include both internal and external resources; ideally, other than a very few "need to know" personnel, the rehearsal should not be planned months ahead as it is unlikely that a true picture will be provided of the state of readiness of the business.

If possible, rehearsals should be conducted at random occasions with different fact scenarios such as loss of critical infrastructures, absence of critical personnel. To be relevant all tests and drills need to be at unexpected times, situations as it is too easy to pass a test where full preparation can be carried out. Ideally the rehearsal should not be overseen / planned by the business's internal personnel who are responsible for implementation of the incident response process.

Are the results of those rehearsals available for review? If recommendations were made (and we have yet to see an IT security report which does not make recommendations), were those recommendations acted upon? The acquirer should drill down into why any recommendations were not acted upon.

There is little value in having a cyber incident policy and procedure unless it is and has been tested in as close a scenario to realism. If there have been no rehearsals and tests, that should be a red (or at least an amber) flag.

6.4.3 Is the company subject to specific data / cyber security laws (e.g. NIST standards, NIS Directive, GDPR etc.); Has it complied with any specific incident reporting obligations under any such laws.

6.4.4 Is the affected company the subject of any existing breach investigation or audits? The acquirer will require to have access to all relevant papers / materials.

6.4.5 Is the affected business the subject of existing undertakings/consent orders in relation to past incidents?

7 PERSONNEL ISSUES

There is little value in a target having carefully and relevantly drafted Policies and Procedures, properly and regularly communicated to employees and others if those who are responsible for the implementation of those Policies and Procedures and for identifying and responding to incidents do not have the technical or business competence to do so.

For that reason, a major part of any evaluation of the cybersecurity status and capabilities of a target must be an evaluation of the personnel who have that responsibility. It need not be solely employees of the target; external contractors can be utilised to provide specialist expertise. However, if the target has chosen to do so, one of the issues to be addressed as part of the process is to ensure that there are no gaps in the capability and that when called upon, all the resources will be immediately available.

For that reason, close examination of the third party support contracts will be an essential part of the analysis. There is limited value in having part of the target's cybersecurity response only available 9 – 5, Monday to Friday. At the very least there must be a mechanism for securing out of hours support on a call off basis without lengthy discussions / arguments on costs.