DOW JONES
RISK AND
COMPLIANCE

The Challenge of Cybersecurity Due Diligence

DOW JONES
RISK AND
COMPLIANCE

The Challenge of Cybersecurity Due Diligence

Rob Sloan,
Head of Cyber Content and Data

Brand reputation is hard won and easily lost and few would deny its importance. Protecting that reputation from undue third party risk is one of the key drivers behind due diligence reports being a standard tool for compliance officers to identify indications of corruption, fraud or other illicit activity among individuals and entities with whom they have (or expect to have) significant direct business dealings.

Working with third parties always involves a degree of risk that increases significantly when the relationship requires entrusting customer or sensitive business data to the other party. In order to thoroughly evaluate the cost/benefit balance for any relationship, risk owners need to be aware of any potential cyber issues in the same way they have long been interested in the potential illegal, immoral or unethical conduct of a third party. Due diligence seeks to identify red flags around internal controls at a company, of which cybersecurity is one.

Organizations should consider complementing their anti¬fraud and anti¬corruption due diligence efforts with research on the effectiveness of cybersecurity controls and the likely threat the business faces from a range of threat actors. There are a number of challenges associated with performing that due diligence, interpreting the results and keeping the research current throughout the lifecycle of a relationship.

THE REQUIREMENT FOR CYBER DUE DILIGENCE

In contrast to the well-defined risks associated with anti-bribery and corruption (for example), cyber risk is broader and oftentimes less obvious. While boards and senior executives are trying to understand the risk to their own data and networks and ensure corporate compliance with a range of regulations affecting different industries, assessing the risk from third parties has regularly been ignored by all but the most forward-facing firms. Cybersecurity incidents arising from external or internal attackers can affect the confidentiality, availability and integrity of data, lead to legal and regulatory penalties, and result in significant reputational damage.

> The Securities and Exchange Commission (SEC) requires all publicly traded companies to notify investors of 'material' cybersecurity risks and incidents.

Organizations regularly collect information regarding network security of suppliers during the Request for Proposal stage, though this information is generally collected to inform technical staff on the practicalities of dealing with the third party and ensuring compliance boxes are checked. The information rarely relates to whether a company has experienced breaches in the past, the impact of attacks and how the organization recovered.

There are three scenarios in particular where performing cyber due diligence is essential:

- In the case of a potential acquisition or merger.
- Where sensitive, business critical or customer data is to be processed or stored with a third party.
- When a client is about to share sensitive, business critical or customer data with your organization.

The risk from connecting two networks together, as often happens following an acquisition, is obvious: the security of both networks becomes weaker due to each adopting the other's shortcomings. Due diligence in this case is to identify cases where enhanced checks (compliance, monitoring, risk assessments) would be required prior to a deal being completed and networks being linked. Network monitoring or remedial action could be recommended as a result of problems raised during due diligence.

Sophisticated threat actors such as states and some organized criminals target data because it has a known value. Hackers will always attempt to get access through the weakest link in the chain: organizations are regularly targeted via their lawyers, accountants, suppliers or PR firms. There has been evidence of third parties being compromised simply to provide a platform for launching attacks into the primary target. If risks are identified at this point, in-depth risk and/or threat assessments are reasonable next steps.

The reverse is also true. In the event that your organization is expected to process or store data for third parties, it is important to understand whether by doing so you are changing the risk profile of your organization and putting proprietary company data or data belonging to existing clients at risk. Organizations carrying out the due diligence should seek to answer three key questions:

- Does the organization have a legal or regulatory obligation to disclose intrusions or data breaches? If yes, is there evidence that they have made disclosures and what do they regard? If no, what assurances

can the organization provide to prove it has taken steps to try and identify security issues?

- Has that organization previously reported any cybersecurity issues and if so, which parts of the business has it concerned, what data was lost and what was the impact?
- Have other companies in the same sector with a similar risk profile been targeted and/or compromised? If yes, what makes the organization under review different?

THE CHALLENGE AS THINGS STAND

There are a number of barriers in carrying out effective cyber due diligence. The first barrier is the diverse set of laws and regulations, or (in many parts of the world) the widespread absence of laws and regulations, that govern when an organization has to disclose that they were the victim of a security breach. Many organizations have experienced data loss incidents, but have never reported them, leaving third parties blind to the risk.

In the United States, 47 states have laws regarding the notification of parties whose personal data has been lost. Very few states publish those breach notifications online and the aim is primarily to prevent identity theft. If other types of information are lost, for example intellectual property or commercial data, there is usually no obligation to notify any authority.

The European Union currently has similarly diverse laws and guidelines, principally focused on fighting identity theft, although the General Data Protection Regulation and the Directive on the security of Network and Information Systems (NIS) seek to change that. When the law comes into force in April 2018, any organization that loses personal data must report it to a competent national authority and the NIS mandates certain types of organization to report cyber breaches, primarily those that form the critical national infrastructure and those that provide communications networks. However, the main focus remains on personal data.

The Securities and Exchange Commission (SEC) requires all publicly traded companies to notify investors of 'material' cybersecurity risks and incidents. This includes not only confirmed data breaches when unauthorized third parties have accessed company data, but also minor breaches carried out by a particularly sophisticated (state) actor even when there is little or no impact. Such information is particularly useful when performing cyber due diligence.

Large parts of the world are completely without any sort of legal or regulatory cover when it comes to disclosing cyber incidents and risk.

There is a lack of publicly available data sources that record breaches and a lack of standardized approaches to capturing breach notification reports. We are constantly reminded by security professionals and the FBI that there are only two kinds of organization – those that have been hacked and those that do not know about it. If this is the case, then there is a serious problem of under-reporting.

ACTIONABLE STEPS

Laws and regulations across the globe will continue to evolve, though the prospect of useful information regarding cyber risks and incidents being available on which to base informed decisions seems some way off. However, there are a number of actions organizations can undertake to address the risk.

The first is to understand the regulatory environment of the target organization. Where do they operate? What data do they hold which would be subject to disclosure regulations? What data is publicly available in official sources such as financial filings?

The second action is open source research to identify previous incidents using as broad a range of source material as possible

and ensuring all of the geographies in which the target organization operates are covered. Some data breaches or attacks will only be covered in specialist press. Others, for example in the case of a disgruntled employee stealing data, may only be covered in local media.

The third action is a continuation of the open source research, but this time expanded to incorporate peers and competitors, especially in the same geographies. Understanding the cybersecurity environment in which the target organization operates may give an indication of whether the sector as a whole is being attacked and what that might mean for data security.

Finally, there are a number of companies that claim to be able to review an organization's cybersecurity passively by probing their network in order to produce a risk score. It is early days for these services, but there is potential to provide indications of risk and, if appropriate, it is worth considering.

CONCLUSION

Organizations are spending millions of dollars on securing their own networks, protecting their critical data assets and providing awareness training to their employees, and yet many are failing to take adequate steps to investigate the cybersecurity reputation and assess cyber risk of companies they will partner and potentially share data with.

A certain amount of knowledge is required to put together research sources and interpret the results (or lack thereof) in the context of an industrial sector or among a group of peer companies, but that then provides a framework to make assessments of any company. The objective is not necessarily to take yes or no decisions, simply to inform the larger due diligence process. All risk can be mitigated, transferred, avoided or accepted, and there is an argument to say that a company that has gone through a data breach incident is better prepared than one that has not. Forewarned is forearmed.

Dow Jones is interested in your requirements for cybersecurity due diligence as well as your experiences and challenges in collecting the information for your own organization.

BIOGRAPHY

Rob Sloan, Head of Cyber Content and Data

Rob publishes a weekly cybersecurity newsletter, provides thought leadership and advises internally on cyber risk. Rob is also a Certified Anti¬Money Laundering Specialist (CAMS).

Starting his career in the UK Government at the Ministry of Defence and later the Foreign and Commonwealth Office, Rob looked at some of the earliest targeted cyber attacks against critical infrastructure before building and leading an incident response and investigation team at a specialist IT security consultancy.

Rob's main interest is the requirements, motivations and technical capabilities of threat actors, particularly nation states.

DOW JONES RISK AND COMPLIANCE

Dow Jones Risk and Compliance is a global provider of risk management and regulatory compliance solutions. With a global team of expert researchers covering more than 60 languages, we deliver enriched risk data, investigative research tools and outsourced services to organizations around the world. Our market-leading data solutions help companies navigate Anti-Money Laundering, Anti-Bribery and Corruption, Economic Sanctions, Third Party Due Diligence, and Commercial Risk operations. Providing compliance professionals with flexible delivery options and a professional services offering, our compliance solutions empower fast and informed decision-making - without compromising on coverage.

For more information,
visit www.dowjones.com/risk

DOW JONES
RISK AND
COMPLIANCE