www.privacyromania.ro

29-30 Ianuarie 2021

PRIVACY ROMANIA 2021

Conferința Națională de Confidențialitate și Protecția Datelor

CYBER AND DATA PRIVACY DUE DILIGENCE, SIMILARITIES AND DIFFERENCES

ASCPD

Asociația Specialiștilor în Confidențialitate și Protecția Datelor

Dan CÎMPEAN

Director General Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, Membru Consiliul Consultativ ASCPD

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO

January 29-30, 2021
PRIVACY ROMANIA 2021
Romanian National Conference on Privacy and Data Protection

Cybersecurity and Data Privacy Due Diligence

By: Dan Cimpean, General Director CERT-RO

30 January 2021 TLP = WHITE

Do you remember ?

- July 2016, Verizon Communications announced that it would pay **4,83 billion USD** in cash to purchase Yahoo!
- January 2017 the price was **cut by 350 million USD** and Yahoo! agreed to pay 50 % of any costs relating to government investigations and private litigation relating to historic data breaches
- Reason: Verizon identified a ma**ssive undisclosed data breach during its due diligence**, which dramatically changed the value of the transaction

Due diligence = a critical aspect of any transaction

- During this process, a purchaser or investor **(the Buyer)** will typically conduct an in-depth review of the corporation to be acquired **(the Target)** to accurately value the transaction
- This due diligence will also form the basis of the representations and warranties that the Target will include in the transaction documents

Importance of due diligence

- Increasingly important aspect of due diligence in today's data- and technology-driven society:
  - cyber due diligence
  - data privacy due diligence
- Once peripheral / minor to a e.g. M&A transaction, they have become critical today

due diligence.

Key issues that practitioners should consider

- When analysing a company's cybersecurity and data privacy practices, look at:

pre-diligence steps

commonly requested diligence items

potential red flags that may signal the need for additional scrutiny

Other issues - Industry

- In US, unlike in Europe, cybersecurity and data privacy are not subject to a single overarching regulatory and statutory framework
- Due diligence requirements may vary depending on the specific industry
- For certain industries, such as healthcare and financial services, it is important that diligence questions focus on the requirements that are unique to those industries

Other issues - Customer / Stakeholder profile

- Having a well-developed understanding of a Target's customer base prior to conducting due diligence is also important
- By identifying the Target's typical customers (e.g., individuals, other corporations, the government), the Buyer can focus diligence requests on the typical data privacy and cybersecurity issues that arise in companies with the identified customer profile

Other issues - Location

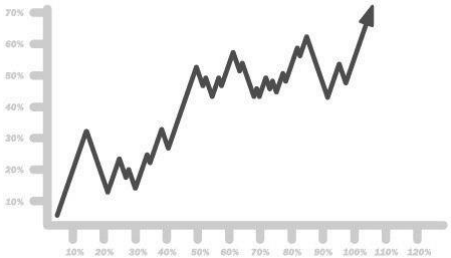
- A **Target** located in EU or that does business with EU customers is likely to be covered by the General Data Protection Regulation (GDPR) and therefore should be subjected to more scrutiny given the large penalties that are authorised under the GDPR

Other issues - Data collection practices

- Understanding the data that a Target typically collects and how it is collected will allow a Buyer to better understand the Target's data privacy and cybersecurity risks
- Care should be taken in analysing any Target that collects a significant amount of PII or receives credit card information, etc.

Other issues - Previous cybersecurity incidents

- A review of historic cybersecurity incidents can help a Buyer understand whether a Target has system vulnerabilities or inadequate policies and procedures, which may indicate unidentified risks
- Certain documents (such as policies and procedures) may warrant more scrutiny for a Target that has a history of cybersecurity breaches and other incidents, and in some cases the Buyer may want to engage in careful technical diligence of the Buyer's system



Historical exposure to cyber & data privacy incidents

- Understanding **historical** cyber and data privacy events is also a major area of focus in due diligence
- Understand whether there are:
  - any pre-existing risks from an earlier breach, or
  - whether there are undisclosed breaches
- Companies are increasingly vulnerable to consumer complaints about how their data is handled

Risks of past or future data breaches

- The **cyber diligence team** typically is:
  - **evaluating any complaints** (including notices of violations and investigations) by individuals and regulatory authorities
  - **reviewing any incident logs that are available**, because the frequency of cybersecurity incidents (whether successful or not) can provide insight into whether the company and its data systems are common targets
  - **reviewing public records** to identify if the Target has been subject to any relevant allegations regarding cybersecurity

Risks of past or future data breaches

- The **data privacy diligence team** typically is:
  - **checking complaints and notices of violations** relating to data privacy issues, such as the failure to respect a data subject's access rights or non-compliance with restrictions on data sharing - such complaints may identify an undisclosed liability, while the frequency of violations and complaints can inform about customers (and other data subjects) acquired
  - understanding the Target's **culture of compliance** with cybersecurity and data privacy requirements

Conducting diligence: contractual obligations and liabilities

- There are two types of contractual relationships that may touch on cybersecurity and data privacy:
  - contracts with service providers
  - contracts with customers

  both of which can create obligations and liabilities that extend beyond those imposed by laws and regulations

Contracts - questions to consider:

- Are there adequate provisions in the agreements to provide comfort to the Target that its data is sufficiently protected?
- Are there any reciprocal requirements imposed on the Target company?
- Are there indemnification or allocations of liability provisions?
- What types of data are being shared or processed? Are there specific obligations that arise from those types of data?
- Are any jurisdictions involved outside that of the Target?

Contracts - questions to consider (cont.):

- Are there any cross-border transfer issues?
- Do third-party vendors and service providers have their own vendors and service providers?
- Are the contracts consistent with any applicable Target vendor management policies?

Contracts - other aspects

- Target company's cyber insurance policies, if such cover exists
- Insurance against data breaches and unintentional privacy violations is becoming increasingly common, both as part of a company's umbrella cover as well as specifically and separately for companies in industries where data is an area of focus
- The policies may provide some comfort by mitigating any identified risks or, conversely, identify areas of greater risk. In conducting this analysis, the Buyer must also confirm that a change of control will not affect the cover

Are we ready for this in Romania ?

- Comprehensive and up-to-date **legislation ?**
- Do we have **capacity**, do we have **knowledge ?**
- More mature public-private-academia partnerships…
- We need to **fill-in the capability-expectations gap…**


CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO
ROMÂNIA

Thank you !!!