Buyer beware

Cybersecurity due diligence for transactions

In the context of a transaction, it is common to focus due diligence on areas such as tax, employment and real estate. Devices enabling connectivity and the adoption of digital technologies (robotic process automation, artificial intelligence, etc.) have increased companies’ vulnerability to a security breach. The connected ecosystem, together with growing regulatory scrutiny of data security, have increased the importance of a cybersecurity due diligence.

Cyber defenses are not impregnable, and cybersecurity concerns are not limited to the technology industry as demonstrated by recent security breaches in the hospitality, airline and health industries. According to the EY Global Information Security Survey 2018-19, 77% of organizations are operating with only limited cybersecurity. Exclusion of cybersecurity due diligence could result in a significant loss of value; worse, it could make it easier for cyber criminals to compromise the security systems of the purchaser.

The value loss could be in the form of theft (of trade secrets, intellectual property or other confidential business data), business shutdowns, regulatory fines, litigation, expenses for forensic and restoration activities, loss of customer trust, and time for crisis management. Cybersecurity due diligence would gather information about:

- Types of high-value digital assets like intellectual property (IP), operations, financial, supplier, customer and plant data, as well as the storage and transfer of data
- Internal rules and regulations — bring your own device (BYOD) policies, identity and access management
- Management, budget and resource allocation for cybersecurity
- Agreements with third parties for data access and the hosting and supply of components, including provisions related to audit and emergency response
- Past breaches
- Risk containment and response-recovery protocols
- Insurance policies
Ideally, cybersecurity due diligence should be performed by a multidisciplinary team consisting of both technical and legal cybersecurity experts who are able to identify, value and reduce the risks. This team would be able to gather information about the target’s risk profile and, more important, interpret the responses and make suitable recommendations to the purchaser. These could include further on-site security assessments, the purchase of cyber insurance, or negotiation of pre-closing covenants, warranties and/or indemnities for discovered and undiscovered issues.

Cyber criminals are moving fast, therefore, it is important for purchasers to manage cybersecurity risks at every stage of the M&A process, including due diligence. Cyber due diligence is an important tool that is available for purchasers to quantify cyber risks – both to assist with deal valuation and to prevent value erosion by protecting digital assets.

“

There are a number of areas where cybersecurity really plays a significant part, both in terms of the ongoing value of an organization and at any point where there is M&A activity. Cybersecurity diligence shouldn’t be seen in isolation – it has to be done in context of the wider business by blending it with financial, operational and technology deal diligence.

Faizul Ali
TAS UK&I Cyber Security Leader

Contacts

Jean-Christophe Sabourin
EY Global Transaction Law Leader
+32 2 774 9990
jean.christophe.sabourin@ey-avocats.com

Peter Katko
EY Global Digital Law Leader
+49 89 14331 25951
peter.katko@de.ey.com

Fabrice Naftalski
EY Global Data Privacy & Cybersecurity Law Leader
+33 1 55 61 10 05
fabrice.naftalski@ey-avocats.com

Mike Maddison
EY EMEIA Cybersecurity Leader, Advisory
+44 20 7951 3100
mike.maddison@ey.com

Faizul Ali
EY UK&I Cyber Security Leader, TAS
+44 20 7951 1172
fali@uk.ey.com

Author

Manu Mohan
EY Law
+32 2 774 9990
manu.mohan@be.ey.com
In an age of M&A complexity, do you pause or proceed?
8 October 2018
By Steve Krouskos
EY Global Vice Chair – Transaction Advisory Services

What corporates and start-ups need from each other
29 March 2018
By EYQ

Recent related thought leadership and information produced by EY include: