Technology Law Analysis

June 20, 2022

CYBER SECURITY DUE DILIGENCE: SHOULD INVESTMENT COMMITTEE AND BOARD MEMBERS CONSIDER THE TARGET'S CYBER SECURITY READINESS BEFORE JUMPING IN?

With the rise in cyber security breaches in the last two years, there is talk of cyber security threats being considered an environmental, social and governance (ESG) concern. Socially responsible businesses are taking measures to protect their systems and their customer data. Failing to do so is not only a reputational risk but could also lead to loss of business as informed consumers may not want to associate with businesses that face frequent security threats.

The government is also taking steps to promote better cyber security practices. Noting the rise in cyber security breaches and the need for a safe internet, the Indian Computer Emergency Response Team (**CERT-In**) has recently issued directions (Directions) imposing strict timelines for reporting of cyber security disputes and other obligations such as maintenance of computer system logs, KYC for customers of data centres, cloud service providers, etc. The Directions introduce penal consequences for non-compliance with its provisions.

In this landscape, investors should be mindful of the level of security measures adopted by by the target as also associated legal compliances. Some items such as frequent past breaches, non-compliance with law with respect to past breaches, etc. could become deal breakers. We discuss some parameters that can be used to determine a business's readiness for cyber security issues.

CYBER READINESS

At present, India has a basic data protection law for "sensitive personal data or information" (SPDI) in the forms of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules)[1] issued under Information Technology Act, 200. SPDI includes information pertaining to passwords, financial info, health data, sexual orientation and biometric information.

The SPDI Rules require entities processing SPDI to implement "reasonable security practices and procedures". Currently, the law does not mandate implementation of any particular security standard but recommends implementing the international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements". However, companies can choose to implement their own standards and remain compliant with the SPDI Rules so long as they implement "comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business."

Investors should therefore ensure that adequate security practices are in place to protect SPDI. It should be noted that SPDI does not cover information such as email addresses and other customer data such as customer preferences, purchase history, etc. which could also be affected as a result of a cyber security breach. Therefore, apart from measures taken to protect SPDI, steps should be taken to protect other types of information and the computer networks as well. The FAQs issued in relation to the Direction by CERT-In also state that organisations need to deploy appropriate security controls and follow reasonable security practices to detect and prevent cyber security incidents.

While the Indian law with respect to data protection and cyber security has not fully developed, keeping the rise in cyber security issues in mind, businesses should adopt comprehensive data protection and security plans. Today, third party vendor assessment forms also include questions on cyber security readiness and therefore adopting such practices is important for business reasons as well. Some of factors that may be relevant when adopting such plans are below:

a. Organization-wide understanding of responsibilities – All members of the organisation, including employees, need to understand what their responsibilities encompass when it comes to ensuring security of systems. Since Covid-19 most organisations have adopted strong employee policies pertaining to use of office computers, removal of data from work computers, confidentiality obligations etc. Such policies are essential to prevent unauthorised use of computer networks and the organisation's data by employees. Companies should also have strong employee exit plans where employees are reminded of their confidentiality obligations. In case of virtual and remote working, multifactor authentication (MFA) platforms should be deployed.

b. Identify risk zones — Businesses must assess their security systems on a regular basis to identify gaps in current security policies. Effective data protection solutions such as measures for protection of firewalls, data encryption, efficient disaster recovery and measures to prevent data loss or erasure should be implemented. Businesses should also keep track of latest vulnerabilities/attacks. The Russian-Ukraine war has given birth to novel chain of

Research Papers

Compendium of Research Papers
January 11, 2025

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Research Articles

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals
January 15, 2025

Key changes to Model Concession Agreements in the Road Sector
January 03, 2025

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

Audio

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper

cyber techniques and created a new paradigm of cyberwarfare. It will not take long for similar tactics to penetrate the corporate world.

c. Visibility and transparency — Businesses should implement data mapping tools to document the types of data records maintained, where it is stored, steps taken to protect data, etc. This information should be available with relevant members of the organisation who may be involved in dealing with any cyber security issues.

d. Implement cyber security policies — A robust policy must be adopted which details the cyber security practices of the organisation including frequency of cyber security audits, employee policies, security measures adopted, etc.

REPORTING PAST BREACHES

The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules) mandates reporting of certain cyber security incidents such as compromise of critical system, unauthorised access of IT systems/ data and several others. As stated above, CERT-In has recently issued Directions to further expand on the reporting requirements. Investors should ensure such reporting has been done and if the target has complied with any guidelines/directions by CERT-In post the attack. Non-compliance with the reporting requirement and with any guidelines/directions issued by CERT-In could result in imprisonment and imposition of a fine.

As per current law, an organisation does not need to inform its users when its affected by a cyber security breach. However, many companies inform users in good faith so that consumers can take measures to safeguard their information. While informing users is not a legal requirement, it should be confirmed if this has been done to avoid surprise legal actions at a later stage from affected users.

CYBER SECURITY INSURANCE

Cybersecurity insurances are gaining relevance in view of the rise in security breaches. An organisation covered by a cybersecurity insurances remains protected financially in case of a breach. Inventors should confirm whether such policies have been obtained and the coverage of such policies. Cybersecurity insurance policies should typically cover situations where the breach has occurred at a third party service provider's end which causes loss of data to the organisation. For instance, breach affecting a healthcare insurance company also affects all companies which obtained healthcare insurance from such company.

CONCLUSION

Readiness to deal with cybercrimes should be an important parameter in due diligences. If lapses are recognised in the diligence, the target can be required to take remedial steps before investment. A cyber security diligence can also help investors identify how prone is the business to cyber risks and help in developing and implementing plans for the future.

– Aparna Gaur, Milind P.M & Gowree Gokhale

You can direct your queries or comments to the authors

[1] Information Technology (Reasonable security practices and procedures and sensitive personal data or information)

on Simplification of registration for FPIs

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024