Crowe

Third-Party Digital Risk

Crowe Advisory Services (India) LLP

Audit / Tax / Advisory

Smart decisions. Lasting value.

What is third-party digital risk

Third party digital risk arises from unauthorised access of entity data and systems, such access enabled by digital security weaknesses of third-parties (customer, supplier, service provider) to whom access has been authorised. This enables an unethical person – competitor, thief, mischief maker, fraudster, to enter your company undetected, via weak third-parties and severely impact your business and assets.

Why does it occur

Business increasingly works through a partner ecosystem covering direct business aspects and / or support operations. The ecosystem must work through technology bases in order to truly deliver value and greater efficiency. Competition is the driver and technology the enabler for digital interaction and automated data-flow integration between businesses and their vendors, customers and service providers.

On the flip-side, the digital interaction opens the door for cyber-risk to creep in via the third parties. The risk increases as third-parties get deeply integrated into the business operations.

Can it occur in my organisation

Third party digital risk can occur in any entity that works in a technology based ecosystem. Your business may be global, national, regional or local; if it is forward looking, it likely embraces (or needs to embrace) technology to effectively integrate third-parties to deliver competitive benefit and efficiency. This creates an actual or potential exposure.

Importantly, your entity could be the offending third party to the ecosystem of another.

We have invested in Security Technologies – we am safe

But have you ensured that third-parties who access your systems and data have similar leval of security? By itself, technology offers limited or no protection.

Policies and Controls governing third-party security need to be properly designed, rigorously implemented and properly monitored. *There must be awareness and discipline, driven by a security conscious culture fostered by top management.*

How does it affect me

Third party digital weakness creates several risks: (a) data loss or misuse - R&D, IP, product, customer, business plans, strategy and the like; (b) asset theft; (c) shutdown or hampered operations with controls in unethical hands, and demands for ransom; (d) data privacy breach with regulatory / contractual non-compliance.

Loss of reputation and business, compensation liability; drop in valuation and corporate consequence of indequate governance follow a breach event. More so if your entity has enabled breach and disruption of another's ecosystem.

But nothing has occurred so far

Luck is very valuable for business. Save the currency of "luck"; don't expend it for protection from third party digital risk. Set up a proper system and monitoring.

Please recognise, that an unethical hacker may have intruded your system or a third-party system and may be biding time for the right opportunity to strike.

The entity is contractually covered

Third party contracts may place responsibility on the counter party. This may help salvage claims liability. However, the loss of reputation, business and assets has occurred for your company; that impact is direct and immediate.

Lack of training to third parties, lack of controls and monitoring over their access and activities, could well nullify the contractual position.

What must we do

A detailed assessment of your systems, policies and controls related to third-party security is needed to assess gaps and risk, develop and implement remediation measures. Periodic updates of the digital risk framework will be beneficial because (a) newer technology is constantly adopted, increasing opportunity for the unscrupulous and risk for the entity; (b) new third parties are joining your ecosystem; and (c) controls implementation tends to dilute over time.

Crowe Advisory Services India can help you manage your Third Party Risks

About Crowe India:

Crowe Advisory Services (India) LLP provides Risk Advisory, Corporate Finance, Taxation, Business Advisory, Digital Security Consulting, Data Sciences and Business Process Outsourcing services. We have offices in eight cities in India.

We are a member of Crowe Global, the eighth largest accounting and consulting network worldwide, with 765 offices across 146 countries.

Disclaimer:

The views expressed herein may not apply to your entity, business, asset or circumstance. Professional advice should be taken, and independent judgment exercised, relative to the engagement scope and related aspects. Further, the opinions expressed herein are not a necessary indicator of our approach to any specific valuation assignment or situation.

Key Digital Security Contacts:

Anil Aravind, Director, Digital Security Services
anil.aravind@crowe.in

Abhijeet Nath, Director, Digital Security Services
abhijeet.nath@crowe.in

Sreejith UG, Cyber Security Lead
sreejith.ug@crowe.in

1105 Embassy Centre,
Nariman Point,
Mumbai 40021

+91 22 6631 1480
www.crowe.in