Business Standard

Work from home: Ensuring data security a challenging task for businesses

Both employers, employees are liable for data breach from home

Sudipto Dey Last Updated at March 29, 2020 20:45 IST

India doesn't have a data protection law or a dedicated law on cybersecurity. Also, there is no specialised law on privacy.

As work from home (WFH) becomes the new normal — at least for the next few weeks — businesses are rushing to put in place more structured WFH policies, say employment law experts.

While business continuity is the primary concern of most corporates, what complicates the matter is the need to ensure the security of client data even in a WFH scenario.

"Companies need to quickly realise that when they are allowing work from home, including mission-critical work, they become intermediaries under the Information Technology Act 2000. Hence, they are duty-bound to comply with the parameters of due diligence and other compliances under the Indian cyber law, rules and regulations," says cyber law expert Pavan Duggal.

India doesn't have a data protection law or a dedicated law on cybersecurity. Also, there is no specialised law on privacy. Experts say this complicates the scenario for businesses as they continue to be liable for breach in client data even when employees work out of the home.

While some employers — mostly in the tech space — already had WFH policies, others had telecommuting agreements. For a majority of businesses, WFH was more of an informal understanding on a case-by-case basis, say experts.

EXPERTSPEAK
RULES & REGULATIONS THAT MATTER

What are key dos and don'ts from employee perspective to safeguard against breach of data while working from home?

Dos:
- Understand and comply with your employer's security policies.
- Ask if you have any doubts regarding the process of printouts and using back-up drives, etc.
- Ensure you use only authorised hardware and software for work.

Don'ts:
- Don't share devices with spouse and children
- Don't be careless with screens and printouts while away from the computer
- Don't forget standard cyber-security tips while keeping anti-virus software up-to-date; don't open attachments from unknown sources

Can an employee face legal action for a data breach from home?

Yes. The laws, especially, the Information Technology Act, 2000, don't distinguish between home and workplace when it comes to data breaches.

Can a staffer claim compensation if he/she contracted Covid-19 while on business travel or at the office?

The principle of 'duty of care' cast an obligation on the employer to take reasonable care in ensuring the safety of its employees.

Where an employer has been complying with the health and safety standards prescribed by the government, it is unlikely for an employee to raise a successful claim for compensation. Also, the burden of proof would be on the employee.

What are the key privacy issues employers should keep in mind while sharing employee data with the government, vendors or other customers?

Currently, it isn't mandatory for employers to share any medical or private information of their employees with third parties. In some states, employers are obligated to report incidents of infectious diseases.

Sensitive personal data should be shared only on a need-to-know basis and personal information should not be published in the public domain.

According to experts from Shardul Amarchand Mangaldas, Trilegal, and Nishith Desai Associates

"Employers have started reviewing their policies and formalising their practices," says Vikram Shroff, head of HR Laws at Nishith Desai Associates. Atul Gupta, partner, Trilegal, points out data confidentiality provisions would apply even while an individual is working from home. "Employers would be advised to remind employees of the same and educate them on best practices to ensure that data continues to remain secure."

Shroff says an employer could initiate legal action for a breach of the employment contract and WFH policy/telecommuting deals.

Take the instance of the $190-billion technology industry in India that employees 4 million people, and is involved in several mission-critical operations for global clients. To transition the bulk of its workforce to work out of home required several regulatory approvals from various government departments, apart from the consent of clients.

"Companies have sought permission from their clients for enabling work from home and built internal crack teams to manage security and privacy issues," says a note prepared by Nasscom. The tech industry is still ironing out some teething regulatory issues with the government, says the industry lobby group.

Experts say companies looking at this transition must immediately first come up with detailed WFH policies, put them up on their websites, and get electronic consent from regular employees. Only those employees who agree with such policies should be allowed to work from home, say experts.

“The company should first ensure they have virtual private networks and cloud solutions so that basic security is taken care of even in a WFM environment,” says G V Anand Bhushan, partner at Shardul Amarchand Mangaldas & Co.

All security protocols that are normally in place relating to not sharing of passwords, shredding of printed documents, not creating back-ups, and not using unsecured networks should be rigorously maintained, he adds.

“Companies have to do far more capacity building among their employees while working from home in these transient times,” says Duggal.