privileged access to existing IT infrastructure facilities, as an urgent or emergency measure. Involvement of third parties increase operational risk, transaction risk and compliance/regulatory risk. Often it is noted that the IT teams have access to UPSI, but are not classified as 'insiders' by organisations, thereby increasing the risk of leakage of UPSI.

4. **Ever connected**: Most employees working remotely, are accessing their organisation's data and networks, even though they are not protected by their organisation's secure IT infrastructure. The financial fraudsters/ cyber criminals are on the prowl, preying on the many rendered as emotionally and financially vulnerable. The fraudsters are employing many methods — some new and some time-tested. They are also quick, using day-to-day developments. The game plan is to make the employee part with information or to install malware in their electronic devices to thieve information.
5. **Emails**: Business email compromise is a huge threat with everyone working remotely. There has been a rise in spear-phishing attacks, that typically involve an employee being convinced to make a change in a standard business process. The perpetrators set up a domain very similar to the corporate domain which have certificates issued, so everything appears to be right. The perpetrators begin sending out email messages stating that there are adjustments to the cloud email infrastructure and as a part of this, they need the employee to reset the access credentials by clicking on the link included. When the employee falls for this, the perpetrators gain access to their email. In effect, the targeted employee becomes the man-in-the-middle between all incoming and outgoing emails. This helps the perpetrators gain access to all the sensitive information of the organisation.

Initiatives to secure UPSI

In order to protect themselves from insider trading or any enforcement action, organisations should take precautionary measures such as evaluating their internal controls and revising the insider trading policies of the organisation, thus ensuring that these policies are clearly demarcating the prohibition of trading on UPSI and adequately addressing the increasing opportunities for such trading that might have been created due to the pandemic. In addition, some of the initiatives that organisations could adopt to secure UPSI are as follows:

- Assess the processes under the 'new normal' to identify areas where the UPSI is more at risk of getting leaked.
- Maintain a structured digital database containing the nature of UPSI and the names of persons who have shared such crucial internal information.
- Minimise circulation of UPSI to attendees and adhere to highest possible standards of data security and confidentiality, while undertaking Board and Audit Committee meetings, on digital platforms.
- Close monitoring of information leakage from official laptops/mobile phone by optimally using the data leakage prevention ('DLP') tools. Consider making information virtual (e.g., paperless environment), without download rights, use of camera, etc.
- Identify additional employees and third parties who are granted access to UPSI on exceptional basis and impose restrictions related to 'Designated Persons'.
- Timely withdrawal of administrative rights and/or other exceptional IT privileges extended to select employees during the lockdown, if any.
- Reiterate (and possibly expand) blackout periods and preclearance of trades for Designated Persons and others in possession of UPSI.
- Remind employees to exercise cyber hygiene and ensure adequate IT preparedness to avoid inadvertent cyberattack and unauthorised access to UPSI.
- Conduct awareness sessions on regulatory requirements to safeguard UPSI and penalties on violation of the Prevention of Insider Trading ('PIT') regulations.

Securing UPSI and ensuring that confidential data does not fall in the wrong hands is critical for an organisation to ensure continued investor confidence, preserving its own reputation and goodwill in the market. Given the growing vulnerabilities to leakages of UPSI and insider trading violations, it is vital that organisations remain proactive in implementing necessary controls and good practices such as investing in the right processes, right technology and people control to prevent potential legal, financial and reputational implications.