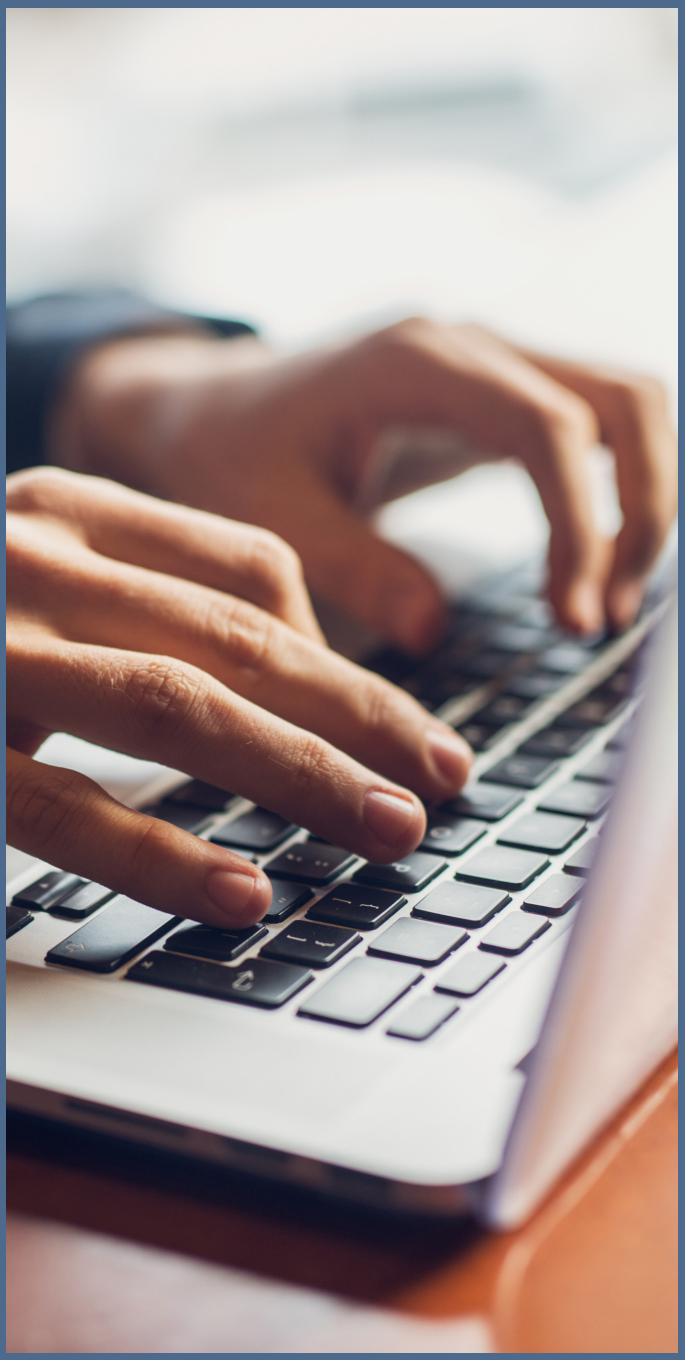


JS|HELD

PERSPECTIVES

Organizational Vulnerabilities in a Protracted Work-from-Home Scenario

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

The beginning of 2020 saw the rapid increase in COVID-19 cases and by mid-2020, the pandemic had spread at such an alarming pace with no vaccine in sight that governments across the globe turned to lockdowns and border closures to contain its transmission. As a result, state, business, and other private institutions had to drastically alter their traditional model of working. With no resumption of 'ops normal' in sight, most organizations adopted a remote working culture, which has persisted even after COVID-19's containment.

The result has been the normalization of work-from-home culture. This has grown largely due to the preference of service professionals for a better work-life balance, the elimination of commuting time, and improved efficiency. Certain organizations were also in favour of the reduced overhead costs, with many moving to smaller offices and hotdesking arrangements in which several workers use a single workstation at different times.

This article, however, delves into the risks of such an unplanned remote working scenario, and discusses why organizations must assess and mitigate the increased risk of employee fraud in the new work environment, where traditional internal controls will be ineffective.

The Paradigm Shift in Work Environment

While COVID-19 dramatically altered the face of the corporate work environment across the board, certain sectors have been more comfortable adopting a remote or hybrid work culture for the long term. Prior to the pandemic, only certain sectors like IT, accounting, and technical services provided employees the flexibility for remote working. But information-sensitive sectors like banking, insurance, healthcare, education, and construction had no or limited room for such arrangements. In November 2020, an analysis conducted by McKinsey's Global Institute in the United States indicated that the finance and insurance sectors have the highest possibility and flexibility of remote working, as depicted in the chart below.[1]

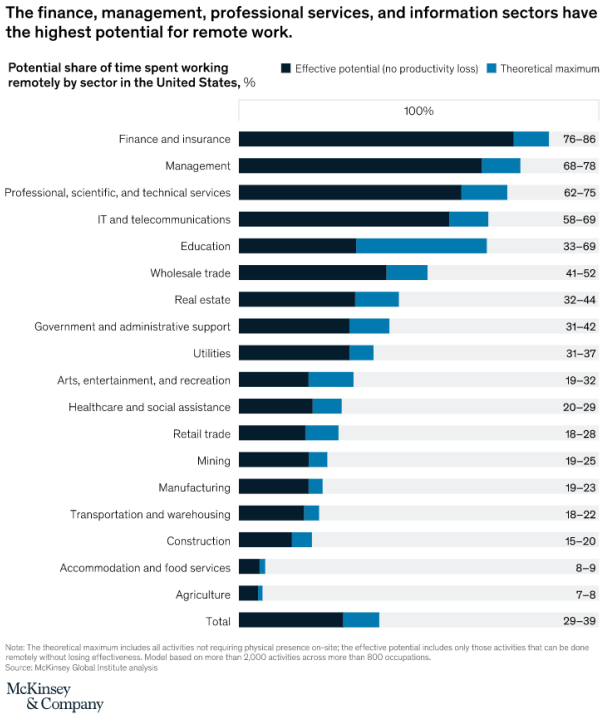


***Figure 1** - McKinsey's Report on What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries, November 2020*

The prolonged work-from-home practice has led corporate employees to reassess their work-life priorities, especially in the wake of mass deaths and the health scare brought on by COVID-19. Many employees relocated to their home cities to be closer to family while several others committed themselves to a dedicated health regime. A CFO Survey conducted by Gartner reveals that post COVID-19, close to 50% of employees prefer remote working.[2]

Higher Flexibility, Lower Oversight = Higher Risk?

Much has been written about work-from-home or the hybrid model being the silver lining of COVID-19, as it made employees and organizations realize that much could be achieved beyond the office walls. However, as we all rejoice at the possibility of less time in traffic, more time for leisure, and better work-life balance, we ought to take a step back and evaluate how this change affects the organization's risk. When organizations plan a major shift in operations, a proper change

[1] https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries
[2] https://www.gartner.com/en/newsroom/press-releases/2021-06-22-gartner-forecasts-51-percent-of-global-knowledge-workers-will-be-remote-by-2021

management protocol must be followed. This requires inputs from risk managers to ensure that the proposed changes do not compromise the safety of the organization or adversely affect its operations.

Since the remote working model was a relatively new construct for a majority of companies that made this shift during the pandemic, no such change management planning was undertaken. However, if companies are considering moving to a remote work or hybrid model on a more permanent basis, such an exercise must be initiated to discover the fault lines that can have catastrophic consequences if left unaddressed. Viewed from a fraud examiner's lens, the shift in work environment leads to higher risk and though these may vary in magnitude by sector and organization, the broader threats include data theft, cybercrime, and occupational fraud, as detailed below.

Data Theft

Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. In today's IT-heavy business environment, organizations prize data as their most valuable asset and consequently, traditional workplaces have built in layers of security for data protection. As the backbone of the world economy, financial services firms especially have stringent data privacy policies and IT systems to protect confidential information. Therefore, prior to the pandemic, most financial institutions were not in favour of remote work, as it may involve accessing sensitive information from outside the company's network. In the midst of the pandemic, however, these organizations had to devise workarounds for employees to access such information from their homes to avoid business interruptions.

Similarly, other sectors also were forced to provide access to company and client data on unprotected public Wi-Fi, home ISPs, and transfer of files between work and personal devices. Sharing of devices, such as laptops, routers, and printers, is also common in a home working environment, and poses an additional threat when roommates or family members work for different organizations. Likewise, with multiple people working from home, the likelihood of co-occupants listening in on sensitive, professional conversations increases. Companies also need to be conscious of data in the hands of untrustworthy employees, who may intentionally misuse data to obtain ill-gotten gains. Any such breach of confidential data could lead to legal implications, loss of customer trust, and reputational damage.

To address this risk, IT departments should consider augmenting security measures with the use of VPNs and require all employees to use secure home networks, create complex passwords, and adjust settings on their computers to lock after short periods of no use. As an additional layer of protection, several firms have also implemented multi-factor authentication and initiated annual training on data security and privacy, including consequences of a data breach. At an organizational level, all employees can be required to read and sign an acceptable use policy for electronic devices, social media, and company data.

Cybercrime

When was the last time you installed that security patch on your home computer? When did you run the last anti-virus program? When does the warranty period lapse on your home printer? Most people would not remember to diligently install security patches and keep up with the latest security updates, despite several email reminders from the IT team. As such, employees unwittingly leave the door open for cyber-attacks. In addition, employees often work long and odd hours from home and have their guards down while tackling professional and personal responsibilities simultaneously. As a result, they may be quick to fall victim to phishing, denial of service attacks, identity theft, and ransomware attacks.

Organizations can test their employees by devising phishing attacks of their own to identify gullible employees, who should be provided targeted training regarding malicious cyber activities. Additionally, IT departments should retain control of software updates and installations such that the individual user cannot override those controls without administrative rights retained by IT. The same should be true for employees that opt for a "bring your own device policy," to ensure company networks and systems are not put at risk by lax security protocols on employees' personal devices.

Occupational Fraud

While data theft and cybercrime are instances of external attack, organizations face the biggest threat from unsupervised employees. Let us now examine the increased risk of fraud due to change in work environment through the lens of a

fraud triangle, which *"states that individuals are motivated to commit fraud when three elements come together: 1) some kind of perceived pressure 2) some perceived opportunity 3) some way to rationalize the fraud as not being inconsistent with one's values."*[3]

1. Perceived Pressure

With the pandemic behind us, businesses have resumed operations with gusto, with competition for market share higher than ever across industries. However, businesses are still recovering from the after-effects of the pandemic, including supply chain disruptions, and loss of long-term contracts, among others. Therefore, not all organizations have been able to revert to pre-pandemic levels of performance bonuses and raises for staff.

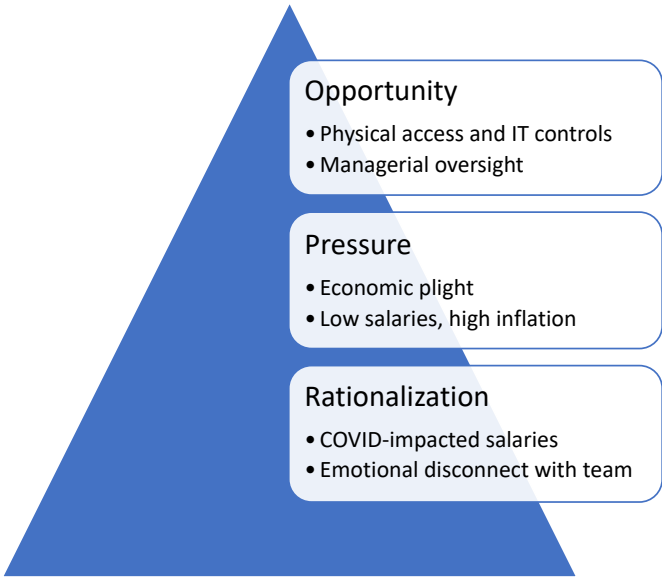
From a macro perspective, the pent-up demand post pandemic and the Russian invasion of Ukraine have driven inflation to record highs across the world.[4] The increased cost of living coupled with marginal, if any, increase in salaries creates financial pressure on employees, who may be tempted to cut a few corners to get ahead of the pack.

2. Perceived Opportunity

A remote working environment opens doors to theft and fraud because physical controls, network access and IT security protocols, and managerial oversight are relaxed. In this work model, companies provide employees with the ability to access confidential data and documents from home, albeit with security measures. However, these controls are not as effective as those at a physical work location, where employees are deterred by CCTV camera, private IP (Intellectual Property) address, and close monitoring by supervisors.

3. Rationalization

COVID-19 took a toll on not just people's health but also their pay checks. Myriads of professionals who were let go during the pandemic have had to take opportunities at lower salaries while others have accepted lower pay with existing employers. In addition, these employees have limited physical interaction and bonding with their teammates and as such, interpersonal rapport and the team connection is weaker than it would have been if they had been working side-by-side at physical offices. Furthermore, physical distance that allows emotional distancing from the larger team or organization also makes it easier for individual employees to rationalize wrongdoing, wherein they justify their actions as a common occurrence, or as a fitting reply for being underappreciated. As mentioned earlier, the post-pandemic era continues to pose financial challenges, which also makes it easier to rationalize obtaining undue financial gain when employees perceive companies to be doing well but not equitably rewarding its workers.



By understanding the pressures, rationalizations and opportunities that can lead to errant behaviour by different levels of staff, anti-fraud professionals can devise practical measures to modify current internal controls and / or develop new means to mitigate the risk of fraud in a remote working environment.

We next delve into the more prevalent occupational frauds in the modified workspace and examine methods to address these risks.

Time Theft

In a remote working environment, managers have little oversight over how employees spend their day. Often, tasks can be completed faster but employees may choose not to inform their superiors, who may then assign additional work to them. This phenomenon is known as time theft, where

[3] https://www.fraud-magazine.com/article.aspx?id=4294999117
[4] https://www.pewresearch.org/fact-tank/2022/06/15/in-the-u-s-and-around-the-world-inflation-is-high-and-getting-higher/

an employee receives pay for working a certain number of hours without having worked for the stated time duration.

One way to curb time theft is to eliminate the temptation by changing the Key Performance Indicators (KPIs) from time-based to achievement-based targets. Instead of setting targets by the staff's experience level alone, managers should actively understand the strengths and weaknesses of their subordinates and set individual targets accordingly. For instance, one employee might be a whiz at Excel spreadsheets and therefore, may be able to complete a data sorting task faster than another employee, who is not as familiar with that software and its functions.

Companies can also consider the following measures and apply those that align with their organizational ethos:

- Managers can schedule routine check-ins with employees to assess if they are on track to meet their goals and if not, investigate why.
- Employees can be asked to work from the office a few days per week to reduce unsupervised time.
- Consider instituting work hours, including scheduled breaks, to replicate the work environment.
- Use technology platforms, like MS Teams, which indicate whether a user is at their workstation or accessing the software from a mobile device.
- Require employees to read and sign documents to indicate compliance with the company's code of conduct, which clearly defines the company's stance on various types of fraud, such as time theft.

Moonlighting

The Cambridge Dictionary defines moonlighting as *"the act of working at an extra job, especially without telling your main employer."*[5] White collar professionals typically will have a clause in their agreement that prohibits them from taking up other employment. In the work-from-home scenario, it is easier to run afoul of this clause and work multiple jobs from the comfort of one's home. However, in doing so, employees risk compromising company data and client information, and could even engage in IP theft, if they work with two competing firms.

Recently, in September 2022, major IT giants in India – Wipro and Infosys – sent a stern communication to their workforces that they will not tolerate moonlighting by employees, with the former even terminating employment of some 300 professionals over allegations of moonlighting. However, India's minister of state for electronics and information technology supported the practice, declaring: *"This is the age of employee-entrepreneurs and companies must now understand there has been a structural shift in the minds and attitudes of the young Indian tech workforce."*[6] In light of such changing trends, companies must consider framing a clear policy on dual employment, specifying the terms and conditions for dual employment, if permitted.

HR and Payroll Fraud

Along with other support functions, Human Resources and payroll functions are also operating remotely. In larger organizations, especially in a white-collar setup, companies may have arrangements where salaries are wire transferred to employee bank accounts. In such instances, the maker-checker system is also embedded within the Enterprise Resource Planning (ERP) software or companies' approval matrices. However, in smaller establishments, salary payments may be via cash or cheque. For cheque payments, remote working hinders the maker-checker system, allowing the person writing the cheque more freedom to tamper with payments. To deter such fraud schemes, companies should consider transitioning to electronic transfer of amounts to employee bank accounts, as these involve negligible costs in comparison to the high cost of fraud. Alternatively, employees in the payroll department can be asked to undertake critical tasks like making and approving salary and other high-value payments from the confines of the office. This is especially applicable when the workforce does not utilize an ERP platform for Human Resources or finance functions.

Similarly, those in Human Resources have a higher chance of colluding with placement agencies that assist with identification of candidates, especially when their conversations are occurring outside the office, and not within earshot of colleagues. To prevent such instances

[5] https://dictionary.cambridge.org/dictionary/english/moonlighting
[6] https://restofworld.org/2022/newsletter-south-asia-moonlighting-indian-law/

of fraud, companies can consider routine, remote monitoring of their emails, wherein forensic data analyses are undertaken to identify suspicious communications. Likewise, it is advised to prohibit employees from communicating with external vendors outside the company's authorized communication systems, which can be monitored. These measures will, at the least, make employees fear that their misconduct may be discovered and, in turn, may act as a deterrent.

CONCLUSION

Remote working was an unplanned detour for most organizations, but this phenomenon is here to stay. Therefore, organizations must evaluate the vulnerabilities of this model and empower its staff with training and tools to effectively thwart the threats of cybercrime and data theft. Companies must also recognize the pressures and opportunities this work environment presents to employees and endeavour to alter oversight measures as well as develop an atmosphere wherein it is difficult for employees to rationalize a deviation from the company ethos. The aim should be to consider this a change management project in reverse, wherein risk mapping and mitigation needs to be undertaken post-implementation.

Acknowledgments

We would like to thank Savita Nair and Vrinda Thakore for providing insight and expertise that greatly assisted this research.

More About J.S. Held's Contributors

Savita Nair is a Managing Director in J.S. Held's Global Investigations Practice. She has led multiple advisory engagements for Fortune 500, private equity, and law firms related to business intelligence, corporate investigations, and litigation support in Asia Pacific and North America. Based in Mumbai, she provides clients with services such as risk consulting, project management, strategic advisory, and organizational development. She is a Certified Public Accountant (inactive), Certified Fraud Examiner, and a Certified Anti-Money Laundering Specialist.

Savita can be reached at snair@jsheld.com or +91 77188 30305.

Vrinda Thakore is an Associate in J.S. Held's Global Investigations Practice in South Asia. Based in Mumbai, Vrinda has experience in fraud and corporate investigations, due diligence, business intelligence, data analysis and process reviews across various sectors. Prior to joining J.S. Held, Vrinda was associated with Indian accounting firms, where her primary focus was fraud and corporate investigations, and matters involving whistle-blower complaints. She has also managed forensic audits and investigations.

Vrinda can be reached at vthakore@jsheld.com.