Retaining Trust In The Virtual World

The post-pandemic shift to hybrid and, sometimes, fully remote working creates new challenges for corporate leaders and management. There are many competing factors involved in working out how to structure any firm's working arrangements. The public debate reflects the varied interests involved, from real estate investors to employers trying to work with new ways of ensuring that client delivery is maintained, but in ways that allow employees to best balance their lives. This is especially important for those with caring responsibilities and those for whom more flexible ways of working enable them to make the best contribution to their workplaces.

The financial services industry has additional concerns to contend with as businesses in this industry continue to iterate their working models. Unlike other industries, the move to remote and hybrid working brings with it compliance requirements. Businesses in the financial services industry have requirements to ensure there are satisfactory arrangements in place to meet regulatory obligations. The expansion of hybrid and remote working has made employee monitoring even more critical and compliance officers have focused on how to best keep track of employee activity in these new settings.

This is not an abstract concern. 73 percent of all teams are expected to have remote workers by 2028, according to CNBC's "How millennials and Gen Z are reshaping the future of the workforce" report. The issue is how can compliance officers keep track of employees in financial services businesses? And how can they do that in a way that meets the demands of regulators, but without being needlessly intrusive?

For certain functions within financial services businesses, employee monitoring is an accepted fact. It is an established compliance activity which financial services businesses implement for purposes such as the prevention and detection of data breaches, employee engagement, increasing privacy and improving unproductive business operations. However, new monitoring technology involving the use of Artificial Intelligence (AI) and Machine Learning (ML) is starting to evolve. As with all new technology it is important to gauge how it improves business processes whilst helping to sustain, rather than degrade, employee trust.

These systems need to be governed by clearly defined monitoring policies. The lack of employee monitoring policies in a company may result in the misuse of employees' private data. This undermines the fundamental right to privacy; businesses and employees must be informed of the relevant regulations in place. Policies also need to keep up with the aforementioned changes in technology. This is important when AI and ML systems can process vast amounts of personal data very quickly. Having policies in place that make it simple for employees to understand what data is being collected, the rationale for that collection and how it is used is vital to ensuring trust.

> According to general employment laws, an employer is permitted to digitally monitor employees

According to general employment laws, an employer is permitted to digitally monitor employees. In the US, Federal and State laws detail how far an employer can go with the employee monitoring programmes. In other jurisdictions such programmes are governed by nationally applicable laws. There are some monitoring processes applicable to most monitoring policies and laws though, for example, if an employee uses a business asset for an activity unrelated to the business, the company does not require any consent to monitor such activity unless the users are informed about the tracking. Employees would also be aware that they are not allowed to use their personal communication networks to communicate work-related details.

Inaccurately crafted employee monitoring policies may breach an individual's fundamental constitutional rights. Precision is key. It's important that businesses are aware of, and compliant with, the relevant laws in those jurisdictions where they operate.

In the US monitoring policies are governed by the Electronic Communications Privacy Act of 1986 (ECPA). This safeguards individuals from unauthorised interception of electronic communications. It limits the ability to read computer transmissions, conduct wire taps and trace telephonic communications and stored electronic communications. Cybersecurity-related investigations are increasing, so it is important to be aware of these laws.

In the EU, it's the General Data Protection Regulation (GDPR) which governs monitoring policies. Most employee monitoring measures are lawful in the EU. However, the practices must be compliant with the provisions of the GDPR. The GDPR holds organisations accountable for protecting the personal information they obtain from employees. It focuses on what data is stored by a company, how the data is updated and how the collected data is protected. The use of stringent and intrusive electronic monitoring techniques however, could have a detrimental effect on staff morale. The GDPR mainly covers the EU, but compliance with the regulation is incumbent upon any organisation that deals with data subjects based in EU member states.

In whichever jurisdiction a financial services business operates, it is important to keep in mind some key principles when setting employee monitoring policies. For example:

- **Determine legitimate reasons:** The reasons for employee monitoring needs to be well defined, to enhance employee cooperation. This could include improving the security of staff and company assets or increase company productivity by monitoring employees' work to facilitate analysis and reporting. The thing that many firms mishandle is the latter. Too often data analysis based on employee monitoring is misunderstood by employees as the employer virtually standing over them, tracking every single action they make.

To guard against damaging trust in the employee-employer relationship, it is vital that monitoring is proportionate whilst meeting regulatory requirements.

- **Maintain transparency:** Employees should be aware that they are being monitored; the stored data, which may include personal information, needs to be kept secure. To the point around analysis, there should also be transparency about how monitoring data is analysed and what corporate actions are linked to the use of that analysis.
- **Have a standard policy:** Employee-monitoring policies should clearly define what employee data is stored and what is not. This protects an individual's fundamental right to privacy.
- **Acquire consent:** Employee-monitoring policies require employee consent. It will ensure they do not keep or save personal information on company-provided laptops or smartphones. The best leaders manage with the buy-in of their people; the worst by corporate fiat.
- **Use of authenticated systems:** The company is responsible for the security of personal data and surveillance recording of employees. Ensuring security while using third-party software or personnel is vital for avoiding misuse of personal data.

The message for employers navigating permanently changed methods of working is that employee monitoring policies need to be updated to reflect these and that new technology can be an aide to ensuring firms in the financial services industry continue to meet or exceed what regulators require. With new technological solutions comes with it a need for more explanation for employees of how these monitor their work product and working patterns. Deployed thoughtfully, employee monitoring policies can help both the employee, their team, and the business, not just to remain compliant with local, national and supranational regulations, but also to optimise the way they work. In doing so, both performance can be assured and employee trust sustained.

AVADHESH DIXIT
Chief Human Resources Officer,
Acuity Knowledge Partners

Avadhesh Dixit is the Chief Human Resources Officer of Acuity Knowledge Partners and also leads the global organisation's CSR activities. He joined the business in 2016 and is based in our Gurgaon office. Avadhesh has 20 years of experience in human resource management at companies in the UK, Ireland, the US, and Europe.

Prior to Acuity, he was Vice President and Head of HR at GE Capital Business Process Management Services Pvt Ltd and the GE Capital-State Bank of India JV. Previously, he held HR leadership roles at CMC Ltd and Tata Consultancy Services Ltd.

He holds an MBA in Human Resources from Delhi School of Economics of the University of Delhi, with a graduate degree in Economics. He is certified as a Global Professional in Human Resources (GPHR) by the Society for Human Resource Management (SHRM), USA, and is a regular speaker at Indian national HR and CSR conferences.

www.linkedin.com/in/avadheshdixit/?ppe=1
E: contact@acuitykp.com