PEER RESPONSE 1

Human-Centred Approaches to Remote Workforce Monitoring in Industry 5.0

This discussion successfully illustrates the challenges that many remote organisations face due to an overreliance on employee monitoring systems, which can shift the focus away from the wellbeing and trust of employees. As O'Connell (2024) emphasises, this erosion of trust creates an imbalance in the power dynamic between employers and staff, potentially leading to disengagement and decreased morale.

A key preventive measure is to involve employees directly in designing the tools used for attendance and task management. As proposed by Anshari et al. (2021), implementing a User-Centred Design (UCD) ensures all stages, from prototype to completed system are grounded in users' needs and experiences. This means gathering continuous feedback, examining market requirements, and incorporating usability testing to prevent discontentment, even when advanced features like facial recognition or geolocation tracking are used.

Mettler and Naous (2022) also highlight that employees should not be treated merely as central data points. Ethical frameworks such as the European General Data Protection Regulation (GDPR) offer clear guidelines for safeguarding employee data, reducing risks of micromanagement-induced stress. Equally important is monitoring mental and psychological wellbeing, which directly impacts productivity and engagement. Galanxhi and Nah (2021) note that remote work often blurs personal and professional boundaries, so monitoring technologies should create a balanced "digital boundary" rather than enforce an 'always-on' culture.

Embedding positive computing principles such as regular feedback loops, promoting job satisfaction, and enabling social participation aligns with Industry 5.0's human-centred vision. Ultimately, your post highlights a timely concern. By adopting trust-based systems and integrating Industry 5.0 principles, organisations can create remote workforce management systems that are not only efficient but also ethical, sustainable, and empowering for employees.

REFERENCES

Anshari, A., Hirtranusi, S.A., Sensuse, D.I. and Suryono, R.R. (2021) 'Designing an Attendance System Model for Work From Home (WFH) Employees Based on User-Centered', International Conference on Computer Science, Information Technology, and Electrical Engineering pp. 125-132.

Galanxhi, H. and Nah, F.F.H. (2021) 'Addressing the "Unseens": Digital Wellbeing in the Remote Workplace' International Conference on Human-Computer Interaction. Cham: Springer International Publishing. pp. 347-364.

Mettler, T. and Naous, D. (2022) 'Beyond panoptic surveillance: On the Ethical Dilemmas of the Connected Workplac' Educational Collaborative for International Schools 2022 Research Papers. Available at: https://aisel.aisnet.org/ecis2022_rp/33

O'Connell, E. (2024) Does Employee Monitoring Infringe on Workers' Right to Privacy, While Working from Home? PHD thesis. National College of Ireland. Available at: https://norma.ncirl.ie/7889/1/elizabethoconnell.pdf (Accessed: 9th August 2025).

PEER RESPONSE 2

Cyber Resilience in Biotech: Lessons from the Evotec Attack and the Promise of Industry 5.0

The Evotec cyberattack is a compelling example of the vulnerabilities that arise from digital dependency in biotechnology, as highlighted by my peer. Given the industry's reliance on advanced research in healthcare and agriculture, it remains a prime target for cyber threats. A commendable step taken by Evotec, as mentioned by Vang (2025), was isolating its servers to enable over 5,000 employees to communicate via a secure domain later migrating the entire infrastructure to a new IT network.

While this reactive strategy was critical, proactive measures are equally essential. One such measure is comprehensive staff training on identifying phishing attempts and ransomware threats, such as suspicious links or email attachments, which should never be opened unless verified (Pope, 2016). Cybersecurity awareness must be embedded into organisational culture.

In addition, adopting a Zero-Trust Security Model is highly advisable. This approach mandates strict verification protocols for all users and devices before granting network access. Systems like endpoint profiling and IEEE 802.1X port-based authentication can significantly reduce unauthorised device connections and potential breaches (Kosaraju, 2025). Laith, Jaouni, and Mihyar (2025) also advocate for robust cyberbiosecurity strategies, including data encryption.

Encrypting sensitive information ensures that even if accessed, the data remains unreadable to unauthorised users. Preventing threats such as SQL injections and cross-site scripting (XSS) via parameterised queries and output encoding is another layer of defense. Ultimately, I agree that Industry 5.0 offers the much-needed balance by integrating intelligent systems with human oversight. Evotec’s experience underscores the importance of both reactive and proactive crisis management in building resilient infrastructures that not only recover but adapt to evolving cyber threats.

REFERENCES

Kosaraju, P. (2025) ‘Safeguarding OT Networks in Biotech Manufacturing Plants’, Journal of Computer Science and Technology Studies 7(3), pp.972-981.

Laith, A.E., Jaouni, H. and Mihyar, A. (2025) ‘Addressing Cyberbiosecurity Challenges in the Modern Era of Biotechnology and Artificial Intelligence: Cyberbiosecurity in the Age of Biotechnology and AI. Global Biosecurity.

Pope, J. (2016) ‘Ransomware: Minimizing the Risks’ Innovations in clinical neuroscience, 13(11-12), p.37.

Vang, T. (2025). Understanding The Impact of Ransomware on Biotechnology. Masters Thesis. California State University. Available at: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=3463&context=etd (Accessed: 7th August, 2025).