

Research Article

The Economics of Distrust: Systemic Risks of Digital Surveillance and Corporate Insecurity in the Modern Enterprise

Partha Majumdar* 

Department of Computer Science, Swiss School of Business and Management (SSBM), Geneva, Switzerland

Abstract

This analysis examines the escalating trend of digital workplace surveillance, arguing that such practices are not tools for operational efficiency but symptoms of a profound crisis of corporate insecurity. Using the late 2025 implementation of aggressive 'bossware' at a major IT services firm as a central case study, the text dissects how granular metrics, such as 300-second inactivity thresholds, reveal a management philosophy that prioritises visible motion over the invisible labour of cognitive work. This approach is situated within a broader ecosystem of surveillance, from the gig economy's invasive monitoring to the algorithmic management of physical labour, demonstrating a sector-wide regression towards outdated control mechanisms. Leveraging psychological frameworks like Self-Determination Theory, the document demonstrates that excessive monitoring shatters the psychological contract between employer and employee, destroying autonomy, competence, and relatedness. This, in turn, fosters a culture of 'performative productivity', incentivising countermeasures like 'mouse jiggling' while suppressing the deep work and creative risk-taking essential for innovation. The central hypothesis posits that this low-trust environment imposes a significant 'surveillance tax'-comprising software costs, management overhead, and high employee turnover-which creates a self-reinforcing 'insecurity loop' of declining performance and increased control. By contrasting this model with high-trust organisations that focus on outcomes rather than inputs, the analysis quantifies the financial dividend of trust, evidenced by superior revenue per employee, lower attrition rates, and enhanced organisational resilience. Ultimately, the text concludes that the path of surveillance, driven by leadership insecurity, is economically unsustainable and a strategic roadmap to obsolescence in an innovation-driven economy.

Keywords

Workplace Surveillance, Organisational Trust, Digital Monitoring Systems, Employee Autonomy, Corporate Productivity Dynamics

1. Executive Summary

The late 2025 revelation that Cognizant, a titan of the global IT services sector, has implemented aggressive "bossware" protocols to monitor employee mouse move-

ments constitutes a watershed moment in the evolving history of workplace management. This report offers a comprehensive, expert-level analysis of the incident, situating it not

*Corresponding author: partha.majumdar@hotmail.com (Partha Majumdar)

Received: 10 December 2025; **Accepted:** 22 December 2025; **Published:** 16 January 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

merely as an operational policy change, but as a symptom of a deepening crisis in corporate leadership—specifically, the crisis of insecurity. By triangulating data from proprietary workforce management tool specifications, recent high-profile corporate scandals (including Wells Fargo, Barclays, and Dell), and robust longitudinal studies on organisational psychology and financial performance, this document validates the critical hypothesis: excessive surveillance is an economic tax imposed by insecure management that ultimately erodes long-term prosperity.

The analysis proceeds through eight exhaustive sections. It begins by dissecting the Cognizant/ProHance case study in granular detail, exposing the disconnect between corporate "process optimisation" narratives and the granular reality of 300-second idleness thresholds. It then expands the scope to the broader "bossware" ecosystem, incorporating the gig economy's draconian monitoring (Upwork/Hubstaff) and the algorithmic management of physical labour (Amazon). The report subsequently leverages Self-Determination Theory and behavioural economic models to demonstrate how surveillance shatters the psychological contract, leading to "performative productivity," the rise of the "mouse juggler" economy, and the suppression of innovation. Finally, by contrasting the "Insecure Enterprise" with high-trust models exemplified by Netflix, Atlassian, and Patagonia, the report quantifies the financial dividend of trust—measured in retention, revenue per employee, and real estate savings—proving that the "insecure" path is statistically correlated with diminished organisational resilience.

2. The Cognizant Paradigm Shift and the Mechanics of Micro-surveillance

The accelerating use of digital monitoring technologies in large organisations has created a profound shift in how work, responsibility, and trust are negotiated between employers and employees. Across the corporate landscape, the rise of granular data capture has begun to blur the boundaries between legitimate operational insight and intrusive behavioural scrutiny. This emerging dynamic signals a deeper tension at the heart of modern knowledge work, where technological capability often advances faster than the philosophies that govern its use.

2.1. The ProHance Implementation: A Granular Analysis of "Idle Time"

In late 2025, the discourse surrounding remote work and employee autonomy shifted sharply following reports that Cognizant had begun rolling out ProHance, a sophisticated workforce analytics platform, across its Indian operations. [18] While the company is one of many in the IT sector to utilise such tools—competitors like Wipro have employed similar systems—the specific configuration and enforcement

protocols revealed in recent disclosures highlight a rigid, mechanistic approach to knowledge work that betrays a profound lack of trust in human capital. [18].

The core of the controversy lies in the specific metrics calibrated within the ProHance system. According to internal reports and employee testimonials, the software is not merely a passive logger of attendance but an active arbiter of engagement. The system is reportedly configured to flag an employee as "idle" if no keyboard or mouse activity is detected for a duration exceeding 300 seconds, or five minutes. [18] If this inactivity persists for 15 minutes, the employee's status is escalated to "away from system," a designation that is logged in the central dashboard and potentially used to calculate "productive hours".

This 300-second threshold is critical to understanding the "insecurity" thesis. In the context of complex software development, systems architecture, or business process consulting—Cognizant's primary domains—a five-minute pause is statistically insignificant as a measure of work cessation. It is, however, highly significant as a measure of cognitive processing. A developer debugging a complex race condition may need to study a static screen of code for twenty minutes; a consultant formulating a strategic response to a client may need to sketch diagrams on paper or think. By setting the tripwire at five minutes, Cognizant's configuration implicitly declares that *motion* is synonymous with *value*. It rejects the invisible labour of thought in favour of the visible labour of peripheral input.

2.2. The Corporate Narrative vs. the Technical Reality

Cognizant's official response to the backlash has been carefully calibrated to frame the initiative as a benign exercise in process improvement. Company spokespersons have asserted that the tools are "not designed or used to track or evaluate the individual performance of employees" but rather to "map client process steps and time metrics to assess process design inefficiencies." The narrative emphasises that this data is aggregated to identify bottlenecks in Business Process Management (BPM) projects and is implemented only with employee consent.

However, a technical analysis of the ProHance suite contradicts this benign framing. The software is marketed with capabilities that far exceed aggregate process mapping. ProHance features include "Asset Optimisation," "Cost of Delivery Optimisation," and "AI-enabled Retention Risk Index." It offers minute-by-minute visibility into active applications, specific web domains visited, and even screen capture capabilities. The dashboard provides managers with a granular view of individual employee behaviours, including "time on & away from system" and "productive time" defined by application whitelisting.

If the objective were solely to identify process inefficiencies—for instance, determining that a specific data entry task

takes too long due to software lag-aggregated data would suffice. The collection of individual-level idle time, down to the granularity of 300 seconds, serves a different function: behavioural modification and control. The "consent" obtained from employees in such asymmetric power dynamics is often nominal; employees are frequently presented with the choice to consent to monitoring or face potential disciplinary action or stalled career progression. Reports suggest that for some executives, the training course to learn ProHance was mandatory, signalling that this is a systemic operational shift rather than a voluntary pilot. [18].

2.3. The Industry Context: A Race to the Bottom

Cognizant is not operating in a vacuum. The move reflects a broader anxiety gripping the legacy IT services sector. As global economic headwinds stiffen and clients tighten budgets, firms are under immense pressure to defend their margins. Cognizant's Q3 2025 revenue guidance projected growth of only 3.8% to 4.8%, suggesting a mature, slow-growth environment where efficiency gains are prioritised over expansive innovation. In such environments, leadership often defaults to cost-cutting and "productivity squeezing."

The adoption of tools like ProHance by Cognizant and Wipro [18] suggests a sector-wide regression to "Taylorism"-the scientific management theory of the early 20th century that treated workers as cogs to be optimised. How-

ever, unlike the physical assembly lines of the Fordist era, where output was tangible and visible, the "assembly line" of the IT sector is mental. The attempt to impose physical-world metrics (movement) onto the mental world (coding/consulting) creates a dissonance that manifests as employee stress and resentment. This is identified as insecurity: confident leaders focus on the *quality* of the deliverable (the code, the report); insecure leaders, unable to judge quality or fearing they are being cheated, focus on the *presence* of the worker.

3. The Anatomy of "Bossware" and the Surveillance Spectrum

To fully appreciate the implications of Cognizant's strategy, one must situate it within the broader ecosystem of "bossware"-a market of surveillance technologies that has exploded in sophistication since the onset of the hybrid work era. These tools range from passive background loggers to invasive systems that capture the intimate details of a worker's home life.

3.1. Taxonomy of Digital Surveillance

Contemporary employee monitoring technologies can be categorised based on their invasiveness and the psychological mechanisms they exploit.

Table 1. The Spectrum of Workplace Surveillance Technologies.

Category	Primary Mechanism	Examples	Intended Corporate Utility	Psychological & Operational Impact
Presence Monitoring	Login/Logout timestamps, badge swipes, VPN connection duration.	Dell RTO Tracking [9], Microsoft Viva.	Attendance verification, real estate utilisation planning.	Creates "Presenteeism"; employees log in early/stay late just to appear active.
Input Telemetry	Keystrokes per hour, mouse distance travelled, idle time detection.	ProHance (Cognizant) [18], Sapience (Barclays). [28]	Granular productivity analysis, billing verification.	High anxiety; disruption of "flow" states; incentivises "mouse jiggling."
Visual/Audio Capture	Random screen screenshots, webcam activation, audio recording.	Hubstaff (Upwork), Teramind.	Proof of work for gig/hourly contracts; data leak prevention.	Extreme privacy violation; sensation of "being watched"; creates hostile environment.
Algorithmic Profiling	Sentiment analysis of chat/email, AI prediction of "flight risk" or unionising.	Amazon "Union Busting" Algos [27], ProHance "Retention Risk."	Pre-emptive HR intervention; security risk mitigation.	"Thought policing"; suppression of legitimate grievance; erosion of trust in HR.

3.2. The Gig Economy Precedent: Upwork and

Hubstaff

The "insecure" management style evident at Cognizant has precursors in the gig economy, where the transaction costs of trust are deemed too high. Platforms like Upwork utilise time-tracking software (often Hubstaff or proprietary equivalents) that takes screenshots of the freelancer's desktop at random intervals-typically every 10 minutes-and logs key-stroke/mouse activity levels.

The horror stories emerging from this sector provide a grim preview of what happens when this logic is applied to full-time corporate employees. Freelancers report having pay deducted because their "activity levels" were too low during specific 10-minute blocks-even if they were reading a document, sketching a design on paper, or thinking through a problem.

- 1) The "Low Activity" Penalty: One freelancer noted that Upwork refunded the client-essentially stealing the worker's wages-because the "low activity" flag disqualified them from payment protection, despite the work being completed.
- 2) The Screenshot Panopticon: The constant threat of a screenshot forces workers to modify their behaviour. They cannot browse Spotify to change a song or check a personal message for fear that the screenshot will capture "non-work" activity at that precise second, leading to a dispute.

This model treats the worker as fundamentally adversarial-a contractor who will cheat unless proven otherwise. By adopting ProHance, Cognizant is effectively importing this "gig economy mistrust" into the salaried enterprise, signalling to long-term employees that they are viewed with the same suspicion as an anonymous temporary contractor.

3.3. Algorithmic Management and Physical Control: The Amazon Case

At the far end of the surveillance spectrum lies Amazon, where monitoring is used not just for productivity but for political control. Reports from 2024 and 2025 indicate that Amazon has employed "intrusive algorithms" to monitor worker interactions and deter union organising activities. [27] The surveillance infrastructure tracks the location and movement of warehouse workers to such a degree that it can identify clustering that might indicate organising conversations.

Furthermore, this surveillance has physical consequences. The relentless pace enforced by algorithmic monitoring-where "time off task" (TOT) is penalised similarly to Cognizant's "idle time"-has been linked to an injury crisis. In 2024, OSHA cited Amazon for exposing workers to ergonomic hazards, driven by the high frequency of lifting and the pressure to meet quotas tracked by the system. [22] The monitoring system creates a feedback loop where the human body is pushed to failure to satisfy the digital metric. This is

the ultimate expression of the "insecure" organisation: one that fears the collective power of its workforce (unions) and the variability of human performance, attempting to crush both through algorithmic rigidity.

3.4. The False Pretext of Security

Proponents of tools like ProHance often retreat to the defence of "security" and "compliance." In highly regulated industries, this is a potent argument. Insider threats are real, and data exfiltration is a liability. However, as the snippets suggest, there is often a "bait and switch." Tools installed for security (e.g., checking for unauthorised USB drives) are repurposed for performance management (checking for 5-minute breaks). [21].

True security focuses on *access* and *anomaly detection* (e.g., why is this user downloading 5GB of data at 2 AM?). It does not require monitoring whether a user moved their mouse at 2:15 PM. When Cognizant uses ProHance to flag "idleness," it is not securing data; it is policing behaviour. The conflation of these two goals allows companies to implement intrusive surveillance under the guise of "cybersecurity best practices," a disingenuous tactic that erodes credibility.

4. The Psychology of Insecure Leadership

There is a direct link between surveillance and "insecurity." This is not merely a colloquial observation but a phenomenon grounded in organisational psychology and leadership theory.

4.1. The Micromanager's Fallacy and Powerless Leaders

Research into the psychology of micromanagement suggests that it stems from a leader's own sense of inadequacy or loss of control. A study by Haselhuhn et al. (University of California) found that individuals who feel powerful are more willing to delegate decision-making authority. In contrast, those who feel "powerless" or insecure in their position are more likely to consolidate control and micromanage. [11].

The transition to hybrid and remote work stripped many traditional managers of their physical proxies for power-the corner office, the ability to "walk the floor," the visual confirmation of subordinates at desks. Facing this void, insecure leaders grasp for digital proxies. The "bossware" dashboard becomes a comfort blanket, providing a stream of data that simulates the feeling of oversight. [25].

- 1) The Illusion of Control: Viewing a dashboard that shows 85% of employees are "active" gives the insecure manager a dopamine hit of control, even if that ac-

tivity is performative. It assuages the anxiety that "people are taking advantage of me." [30].

- 2) Lack of Trust as a Projection: Managers who do not trust themselves to lead through inspiration or outcome-measurement often project that untrustworthiness onto their teams. They assume that because *they* would slack off without supervision, their team must be doing the same.

4.2. Self-determination Theory and the Psychological Contract

The imposition of strict surveillance violates the fundamental tenets of Self-Determination Theory (SDT), which posits that human motivation relies on three psychological needs: Autonomy, Competence, and Relatedness. [2].

- 1) Autonomy: The 300-second idle rule explicitly destroys autonomy. The worker no longer owns their time; the algorithm does. They cannot choose to take a walk to solve a problem; they must wiggle the mouse. This loss of agency is a primary driver of burnout and disengagement. [18].
- 2) Competence: Surveillance sends a clear signal: "We do not believe you are competent enough to do your job without constant supervision." This insults the professional dignity of skilled workers (like the engineers at Cognizant), leading to a "set-up-to-fail" syndrome where the employee internalises this lack of faith. [12].
- 3) Relatedness: The manager transforms from a mentor/coach into a warden/auditor. The relationship becomes transactional and adversarial. The "parasocial" relationship with data replaces the human relationship, as managers manage spreadsheets of activity rather than people.

4.3. Stress Proliferation and the Privacy Violation

The psychological toll of this environment is measurable. The concept of "stress proliferation" suggests that the primary stressor (surveillance) spawns secondary stressors, such as the fear of job loss, the invasion of privacy, and the inability to decompress. [18].

- 1) Privacy as a Mental Health Bastion: In a home office, the boundary between "work" and "life" is permeable. Surveillance tools that take screenshots or track activity blur this line aggressively. Employees live in a state of hyper-vigilance, fearing that a family member walking into the room or a personal notification popping up might be captured and penalised. [5].
- 2) The Cognitive Tax: The constant awareness of being watched imposes a "cognitive tax." A portion of the worker's brain is always dedicated to monitoring the monitor-"Has it been 4 minutes? Should I move the mouse?"-leaving less processing power for the actual

work. [19].

5. The Counter-measures and the Efficiency Paradox

The implementation of surveillance creates an adversarial game. According to Goodhart's Law, "When a measure becomes a target, it ceases to be a good measure." By making "mouse movement" the target, Cognizant has effectively incentivised "mouse movement" rather than "software development."

5.1. The Rise of the "Mouse Jiggler" Economy

The most immediate market response to surveillance is the proliferation of "mouse jiggers"-hardware devices or software scripts designed to simulate activity.

- 1) The Wells Fargo Incident: In 2024, Wells Fargo fired over a dozen employees for using "simulation of keyboard activity" devices. The bank caught them, but the incident reveals the flaw in the metric. If the employees were meeting their outcomes, the juggler shouldn't have mattered. If they weren't, the lack of output should have been the red flag, not the input simulation.
- 2) The "Jugaad" Resistance: Following the Cognizant news, internet forums lit up with employees sharing "jugaad" (improvisational hacks). Techniques range from placing an optical mouse on a ticking wristwatch (the second hand triggers the sensor) to using "auto-typer" scripts that simulate keystrokes at random intervals. [20].

This "Cat and Mouse" game represents a massive diversion of human ingenuity. Highly intelligent engineers are deploying their skills to defeat the ProHance algorithm rather than to defeat the company's competitors. The "insecure" company inadvertently turns its workforce into an internal red team, constantly probing the management system for vulnerabilities rather than focusing on client value.

5.2. The Disruption of Deep Work and Flow

The 5-minute idle threshold is scientifically hostile to high-performance cognitive work. Computer science research and the concept of "Flow" (Mihaly Csikszentmihalyi) dictate that deep concentration requires uninterrupted immersion.

- 1) The Cost of Interruption: It takes an average of 23 minutes to return to a task after an interruption. [17] By forcing an employee to break focus every 5 minutes to interact with the peripheral, the surveillance tool perpetually prevents the attainment of deep flow.
- 2) Shallow Work Incentives: The system rewards "shallow work"-answering emails, moving tickets in Jira, and constant clicking. It punishes "deep work"-staring at code, sketching architecture, reading documentation.

Over time, the organisation's output shifts toward the shallow: lots of activity, very little breakthrough innovation.

5.3. The Suppression of Creativity

Creativity is inherently inefficient and non-linear. It often involves periods of apparent inactivity or "browsing" that might be flagged as "non-productive" by a tool like ProHance. Research indicates that close monitoring significantly dampens intrinsic motivation, which is the fuel for creativity. [2].

- 1) Risk Aversion: Employees under surveillance become risk-averse. They stick to known methods that generate constant, visible activity. They avoid experimenting with new tools or approaches that might require a learning curve (which looks like slowness to the algorithm). [19].
- 2) The "Innovation Tax": In an industry like IT services, where margins are maintained by moving up the value chain to high-end consulting and AI implementation, suppressing creativity is fatal. The "insecure" company optimises the present process at the expense of future invention.

6. Comparative Case Studies of Control

Cognizant is part of a constellation of companies that have attempted-and often failed-to assert control through surveillance.

6.1. Barclays: The "Big Brother" Backlash

Barclays Bank provides a cautionary tale. The bank installed Sapience Analytics (a functional peer to ProHance) to track desk time and send automated warnings to staff who spent too much time "out of the zone." [28].

- 1) The Mechanism: The system tracked toilet breaks and water cooler visits, labelling them as "unaccounted activity."
- 2) The Fallout: Whistleblowers described a culture of fear where employees were terrified to step away. The "stress was beyond belief." [28].
- 3) The Retreat: Following intense media scrutiny and pressure from privacy groups, Barclays was forced to scrap the system. [16] The reputational damage branded the bank as a "dystopian" employer, likely impacting its ability to recruit top fintech talent.

6.2. Dell: The RTO Badge Tracking Disaster

In 2024, Dell attempted to enforce a Return-to-Office mandate through rigorous tracking of badge swipes and VPN connections.

- 1) The Policy: Employees were colour-coded based on

their on-site presence. Remote workers were explicitly told they would be ineligible for promotion, creating a two-tier caste system. [9].

- 2) The Revolt: The policy led to a collapse in employee engagement scores (eNPS). Despite the threats, nearly 50% of the workforce reportedly disregarded the mandate, exposing the limits of coercive control. [14] Dell's leadership, insecure about their command over a distributed workforce, engaged in a power struggle they could not win, damaging morale without achieving the desired compliance.

6.3. EY: The "Compliance" Purge

Ernst & Young (EY) fired dozens of employees in 2024 for watching multiple training videos simultaneously during a "learning week." [8].

- 1) The Trap: The employees were trying to meet mandatory continuing education credits. The system allowed multiple streams, but the company later classified this as an ethical breach.
- 2) The Interpretation: This incident highlights the rigidity of the surveilled workplace. In a high-trust environment, an employee multitasking during training might be seen as eager or efficient (or the training might be seen as poorly designed). In a low-trust, compliance-heavy environment, it is a firing offence. This creates a culture where "following the rules" (even poorly defined ones) is more important than learning or intent.

7. The Economic Argument for Trust (The "Secure" Model)

The assertion that "a company that does not believe in its employees can never prosper" is strongly supported by financial and operational data. Trust is not merely a "soft skill"; it is a hard economic asset with a measurable return on investment (ROI).

7.1. The High Cost of Distrust

The "Trust Tax" is real. Gallup's "State of the Global Workplace" report (2024) estimates that disengaged employees-a direct byproduct of low-trust management-cost the global economy \$8.9 trillion, or 9% of global GDP. [29].

- 1) Turnover Costs: The cost to replace a skilled employee (like a Cognizant engineer) is approximately 200% of their annual salary. [26] Surveillance-induced churn bleeds capital.
- 2) Transaction Costs: In economics, trust reduces transaction costs. When trust is low, every interaction must be verified, monitored, and audited. The cost of the ProHance license, the managers' time spent reviewing the "idle" reports, and the HR time spent on disciplinary hearings are all "transaction costs" that high-trust com-

petitors do not pay.

7.2. The High-trust Dividend: Comparative Financials

Contrasting the "Insecure" model with "Secure" organisations reveals a stark performance gap.

Table 2. Financial and Operational Metrics of High-Trust vs. Low-Trust Organisations.

Metric	High-Trust Model (e.g., Netflix, Atlassian, Patagonia)	Low-Trust Model (e.g., Cognizant, Dell, Wells Fargo)	Economic Impact
Revenue Per Employee	Netflix: ~\$3.10M. [15] Atlassian: High efficiency reported.	Legacy IT: Typically \$50k-\$100k. Dell: Revenue shrank 11-14% in 2023/24. [6]	Trust enables higher leverage of human capital.
Turnover Rate	Patagonia: <4%. [4] Atlassian: High retention via flexibility. [3]	Retail/IT Avg: Often >15-20%. High voluntary attrition due to RTO/Surveillance.	Low turnover saves millions in recruitment/training.
Real Estate Costs	Atlassian: "Team Anywhere" saved meaningful capital on office space. [10]	Dell: High sunk costs in offices; forcing RTO to justify real estate.	Distributed trust allows capital reallocation to R&D.
Productivity Metric	Outcomes (subscribers, features, sales).	Inputs (badge swipes, mouse moves, idle time).	Outcome-focus drives value; Input-focus drives waste.

- 1) Netflix: Operates on "Context, Not Control." [23] They do not track hours or vacation. This attracts "fully formed adults" who drive massive revenue per head. [24] Their \$3.10M revenue per employee is among the highest in the world, a direct result of a culture that refuses to micromanage. [31].
- 2) Atlassian: The "Team Anywhere" policy allows 40% of staff to live remotely. Internal data showed *no dip in productivity* and higher employee engagement. They save huge sums on real estate, which is reinvested in product development. [3].
- 3) Patagonia: With a turnover rate of less than 4%, Patagonia defies the retail industry norms. [1] Their policy "Let My People Go Surfing" is a statement of ultimate trust: we trust you to manage your time. This results in a fanatically loyal workforce that stays for decades, preserving institutional knowledge and reducing costs. [4].

8. The Ripple Effects: Legal, Brand, and Future Viability

The decision to embrace surveillance has consequences that extend beyond the immediate P&L statement.

8.1. The "Adverse Selection" in Recruitment

Companies like Cognizant face an "adverse selection"

problem in recruitment. In a transparent job market (Glassdoor, Reddit, Blind), the "mouse tracking" news is a scarlet letter. Top-tier engineers-who have options-will avoid these firms.

- 1) The Talent Drain: The most creative, autonomous, and valuable workers will self-select out of the applicant pool.
- 2) The Residual Workforce: The company will be left with workers who have fewer options or who are willing to tolerate indignity-or, worse, workers who specialise in "gaming the system" rather than doing the work.

8.2. Regulatory and Legal Risks

The legal landscape is tightening.

- 1) Unionisation Risks: As seen with Amazon, intrusive surveillance is a major driver of unionisation efforts. Workers organise to protect themselves from the algorithm. [27] The NLRB is increasingly hostile to surveillance used to chill protected concerted activity. [13].
- 2) Data Privacy (GDPR/CPRA): As surveillance moves into the home (via remote work), the line between "work data" and "private data" blurs. Capturing a screenshot of a desktop that might have a personal medical email open exposes the company to massive liability under GDPR and other privacy frameworks.

8.3. The "Trust Gap"

PwC data shows a widening "trust gap": 86% of executives think employees trust them, but only 67% actually do. [7] Policies like ProHance blow this gap wide open. Once trust is lost, it is incredibly expensive to regain. Future initiatives-whether strategic pivots, restructuring, or new product launches-will be met with cynicism and resistance by a workforce that feels the company views them as the enemy.

9. Strategic Conclusion: The Insecurity Loop vs. the Prosperity Cycle

The deployment of tools like ProHance by Cognizant and similar measures by Dell and Wells Fargo serves as a diagnostic marker for organisational insecurity. It reveals a management layer that does not know how to measure value, only volume.

This insecurity triggers a destructive Insecurity Loop:

- 1) Management Fear: Leaders fear losing control in hybrid setups.
- 2) Surveillance Imposition: Tools track input (mouse moves) rather than output.
- 3) Erosion of Trust: Employees feel infantilised; the Psychological Contract is broken.
- 4) Performative Compliance: Employees use "jigglers" or waste time "looking busy" (The Productivity Theatre Tax).
- 5) Data Distortion: Management receives bad data (fake activity), reinforcing the need for *more* surveillance.
- 6) Talent Exodus: High performers leave; the company stagnates.

Conversely, the Prosperity Cycle (Netflix/Patagonia) works in reverse:

- 1) Management Trust: Leaders set context and goals.
- 2) Autonomy: Employees control their "how" and "when."
- 3) High Engagement: Intrinsic motivation drives discretionary effort.
- 4) Innovation: Safe to experiment and fail.
- 5) Retention: Talent stays; institutional knowledge compounds.
- 6) Prosperity: High revenue per employee and organisational resilience.

10. Final Verdict

A company that does not believe in its employees imposes a "surveillance tax" on itself-paying for software to track work, paying managers to watch the software, and paying to replace the employees who leave because of it. In the highly competitive, innovation-driven economy of the 2020s, this tax is too high to bear. Cognizant's retreat into the metrics of the factory floor-measuring the movement of the mouse rather than the movement of the mind-is not a strategy for

prosperity, but a roadmap to obsolescence.

Abbreviations

BPM	Business Process Management
CPRA	California Privacy Rights Act
eNPS	Employee Net Promoter Score
GB	Giga Byte
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HR	Human Resources
IT	Information Technology
NLRB	National Labour Relations Board
P&L	Profit and Loss
RTO	Return to Office
SDT	Self-Determination Theory
TOT	Time Off Task
VPN	Virtual Private Network

Author Contributions

Partha Majumdar is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

- [1] Ardill, L. (2023, October 17). Culture Swipe: Patagonia, Point Break & Tiny Turnover Rates. Retrieved November 30, 2025, from <https://www.workvivo.com/blog/patagonia-values-culture-turnover/>
- [2] Arnaud, S., & Chandon, J. L. (2014, January 15). Will monitoring systems kill intrinsic motivation? An empirical study. Retrieved November 30, 2025, from <https://shs.cairn.info/revue-de-gestion-des-ressources-humaines-2013-4-page-35?lang=en>
- [3] Atlassian (2023, June 13). Well-executed distributed work makes for happier, more productive teams. Retrieved November 30, 2025, from <https://www.atlassian.com/blog/teamwork/distributed-work-research>
- [4] Aziz, A. M., & Osman, Z. (2025, January 1). Conceptual Framework Development of Employee Productivity among the Employees in Electrical and Electronic Manufacturing Industry. ResearchGate. Retrieved December 20, 2025, from <https://hrmars.com/IJARBS/article/view/23479/Conceptual-Framework-Development-of-Employee-Productivity-among-the-Employees-in-Electrical-and-Electronic-Manufacturing-Industry>

- [5] Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, 51(1), 87–106. Retrieved December 20, 2025, from <https://www.tandfonline.com/doi/full/10.1080/00236561003654776>
- [6] Battle, P. (2024, May 11). Dell will begin tracking its employees to enforce a harsh new policy. Retrieved November 30, 2025, from <https://hermistonherald.com/2024/05/11/dell-will-begin-tracking-its-employees-to-enforce-a-harsh-new-policy/>
- [7] Berrone, P., & Gomez-Mejia, L. R. (2009, February 1). Environmental Performance and Executive Compensation: An Integrated Agency-Institutional Perspective. ResearchGate. Retrieved December 20, 2025, from https://www.researchgate.net/publication/278305114_Environmental_Performance_and_Executive_Compensation_An_Integrated_Agency-Institutional_Perspective
- [8] Broomfield, B. (2024, October 23). 'Just cruel' | Fired EY employees hit back after losing jobs for watching multiple training videos at once. Retrieved November 30, 2025, from <https://www.hrgrapevine.com/us/content/article/2024-10-23-fired-ey-employees-hit-back-after-losing-jobs-for-watching-multiple-training-videos-at-once>
- [9] Broomfield, B. (2024, September 30). Dell tells sales staff to return to office five days a week. Retrieved November 30, 2025, from <https://www.hrgrapevine.com/us/content/article/2024-09-30-dell-tells-sales-staff-to-return-to-office-five-days-a-week>
- [10] CRE Analyst (2024, October 1). Atlassian's 100% Remote Model: A Case Study in Office Space Reduction. Retrieved November 30, 2025, from <https://www.creanalyst.com/insights/atlassians-100-remote-model-a-case-study-in-office-space-reduction>
- [11] Deen, C. M., Kiewitz, C., Kim, J. Y., Restubog, S. L. D., Chih, Y. Y., & Tang, R. L. (2025). Helicopter bosses: Development and validation of the micromanagement scale. *Journal of Management*. Retrieved December 20, 2025, from <https://doi.org/10.1177/01492063251378092>
- [12] Dogru, C. (2021, December 1). The Effects of Electronic Surveillance on Job Tension, Task Performance and Organizational Trust. ResearchGate. Retrieved December 20, 2025, from https://reference-global.com/article/10.2478/bsrj-2021-0023?utm_source=researchgate.net&utm_medium=article
- [13] Dungan, R. (2024, October 25). Feds warn employers about overstepping the mark with employee monitoring. Retrieved November 30, 2025, from <https://www.hrgrapevine.com/us/content/article/2024-10-25-feds-warn-employers-about-overstepping-the-mark-with-employee-monitoring>
- [14] Employment Practices Solutions (2024, March 7). Dell Employees Disregard Return to Office Incentives. Retrieved November 30, 2025, from <https://www.epspros.com/news-resources/news/2024/dell-employees-disregard-return-to-office-incentives.html>
- [15] Finbox (2025, November 28). Revenue Per Employee for Netflix Inc. Retrieved November 30, 2025, from https://finbox.com/NASDAQGS:NFLX/explorer/total_rev_to_employees/
- [16] Finextra (2020, February 21). Barclays pulls plug on Big Brother. Retrieved November 30, 2025, from <https://www.finextra.com/newsarticle/35327/barclays-pulls-plug-on-big-brother>
- [17] Gagne, M., Forest, J., Gilbert, M. H., Aube, C., Morin, E. M., & Malorni, A. (2010, August 1). The Motivation at Work Scale: Validation Evidence in Two Languages. ResearchGate. Retrieved December 20, 2025, from https://www.researchgate.net/publication/230846109_The_Motivation_at_Work_Scale_Validation_Evidence_in_Two_Languages
- [18] Glavin, P., Bierman, A., & Schieman, S. (2024, March 28). Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being. Retrieved December 20, 2025, from <https://pmc.ncbi.nlm.nih.gov/articles/PMC11300163/>
- [19] Kamarudin, N., Nizam, N. Z., & Sani, A. M. (2022, April 1). THE IMPACT OF MICROMANAGEMENT ISSUE AMONG MANUFACTURING INDUSTRY: EMPLOYEES PERCEPTION AND JOB SATISFACTION. ResearchGate. Retrieved December 20, 2025, from https://www.researchgate.net/publication/359850380_the_impact_of_micromanagement_issue_among_manufacturing_industry_employees_perception_and_job_satisfaction
- [20] Kayas, O. G. (2023, November 1). Workplace surveillance: A systematic review, integrative framework, and research agenda. ScienceDirect. Retrieved December 20, 2025, from <https://www.sciencedirect.com/science/article/pii/S0148296323005714>
- [21] Konjen, H. (2025, November 18). Algorithmic Management and the Future of Human Work: Implications for Autonomy, Collaboration, and Innovation. Arxiv. Retrieved December 20, 2025, from <https://arxiv.org/html/2511.14231v1>
- [22] McClure, M., & Godinez, V. (2023, February 1). US Department of Labor finds Amazon exposed workers to unsafe conditions, ergonomic hazards at three more warehouses in Colorado, Idaho, New York. Retrieved November 30, 2025, from <https://www.dol.gov/newsroom/releases/osh/osh20230201-0>
- [23] Milmo, D. (2024, June 14). US bank Wells Fargo fires employees for 'simulating' being at their keyboards. Retrieved November 30, 2025, from <https://www.theguardian.com/business/article/2024/jun/14/us-bank-wells-fargo-fires-employees-keyboards>
- [24] Narragon, R. (2025, June 11). How the Atlassian System of Work connects distributed teams. Retrieved November 30, 2025, from <https://www.atlassian.com/blog/work-management/how-the-atlassian-system-of-work-connects-distributed-teams>

- [25] Netflix (n.d.). The Best Work of Our Lives. Retrieved November 30, 2025, from <https://jobs.netflix.com/culture>
- [26] Paul, J. (2025, November 19). Cognizant To Monitor Employee's Keyboard & Mouse Activity? Netizens Share hilariously Brilliant 'Jugaad' (And Memes). Retrieved November 30, 2025, from https://in.mashable.com/culture/102672/cognizant-to-monitor-employ-ees-keyboard-mouse-activity-netizens-share-hilariously-brilliant-jugaad-a#google_vignette
- [27] PwC (2024, March 12). PwC's 2024 Trust Survey: 8 key findings. Retrieved November 30, 2025, from <https://www.pwc.com/us/en/library/trust-in-business-survey.html>
- [28] Sainato, M. (2024, May 21). 'You feel like you're in prison': Workers claim Amazon's surveillance violates labor law. Retrieved November 30, 2025, from <https://www.theguardian.com/us-news/article/2024/may/21/amazon-surveillance-lawsuit-union>
- [29] Saraiva, M., & Nogueiro, T. (2025, February 1). Perspectives and Realities of Disengagement Among Younger Generation Y and Z Workers in Contemporary Work Dynamic. ResearchGate. Retrieved December 20, 2025, from https://www.researchgate.net/publication/389103701_Perspectives_and_Realities_of_Disengagement_Among_Younger_Generation_Y_and_Z_Workers_in_Contemporary_Work_Dynamic
- [30] Silvester, A. (2020, February 20). Barclays installs Big Brother-style spyware on employees' computers. Retrieved November 30, 2025, from <https://www.cityam.com/exclusive-barclays-installs-big-brother-style-spyware-on-employees-computers/>
- [31] World Economic Forum (2023, December 12). Patagonia - Sparking the sustainability cultural shift at every level. Retrieved November 30, 2025, from <https://initiatives.weforum.org/industry-net-zero-accelerator/case-study-details/patagonia---sparking-the-sustainability-cultural-shift-at-every-level/aJYTG00000001H34AI>