Navigating the Misfit Between Rigid Security Standards and Human Activity Systems

Moufida Sadok[1*]

[1] *School of Criminology and Criminal Justice, University of Portsmouth, UK*

Abstract

Information Security Management (ISM) remains dominated by a tech-centric paradigm that treats cybersecurity as a hard engineering problem solved through technical artefacts and rigid compliance patching. This view overlooks the reality that organisations operate as complex Human Activity Systems. This paper evaluates the systemic misfits between formal security controls and real-world work practices. Synthesising data from multi-year insights including the UK Cyber Security Breaches Survey, Verizon Data Breach Investigations Report (DBIR), ENISA Threat Landscape, and the World Economic Forum Global Cybersecurity Outlook, the paper illustrates a compounding accumulation of technical vulnerability debt alongside widespread failures in asset management. This structural friction triggers a behavioural backlash: when top-down, rigid security policies restrict operational workflows, well-meaning employees actively deploy workarounds, including unmanaged "*Shadow AI*" systems, to preserve business productivity. We argue that effective security cannot be achieved by enforcing compliance with sterile, off-the-shelf templates. Instead, we propose a holistic framework that positions front-line users and local operational context as core elements of system design and implementation, ensuring that security controls support, rather than sabotage, everyday legitimate work.

Keywords

Socio-Technical Systems; Human Activity Systems; Information Security Management; Security Workarounds; Participatory Co-Design; Shadow AI.

1. Introduction: The Socio-Technical Reality of Cybersecurity

Cybersecurity in organisational practice is frequently mischaracterised as a purely technical issue. This narrow view prioritises the deployment of hardware, software, and telecommunication components while neglecting the human and procedural elements that animate these systems. Exceptionally rigid engineering perspectives overlook the core reality that an Information System (IS) relies fundamentally on interrelated components supported by human actors and operational procedures [33, 38]. Managing security risks through a strict technical lens creates severe operational difficulties because risks do not exist in a vacuum; they manifest within complex organisational systems across fluid functional domains like sales, manufacturing, finance, and human resources. Confronting this complexity requires reclaiming and asserting that a system's social and technical dimensions are inextricably intertwined and

STPIS2026: Proceedings of the 12th International Conference on Socio-Technical Perspectives in IS, September 16-17th L'Aquila, Italy

* Corresponding author.

moufida.sadok@port.ac.uk (Moufida Sadok)

0000-0003-2981-6516 (Moufida Sadok)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-10

CEUR-WS.org/Vol-4325/paper30.pdf

must be optimised jointly rather than in isolation [45]. Managing risks across this complex landscape requires a dedicated socio-technical approach. Without it, a critical user-designer communication gap emerges, leading to a profound misfit between rigid technical security controls and the real-world working practices of the people who use them.

This friction underscores a long-standing structural reality in information systems: solving the 'human factor' in security cannot be achieved by forcing compliance with rigid technical architectures, but instead requires frameworks that treat human behaviour and local operational context as core components of system design [12]. This highlights the necessity of treating an information system as inherently social, where security architectures must support complex, intra-individual sense-making dimensions of localised actors [10]. As Henshaw and Mhajne [27] point out, cybersecurity as a concept is inherently fluid, yet institutional definitions remain constrained by a narrow focus on securing the structural infrastructure of systems, networks, and data. By defining security strictly through this technical lens, organisations systematically separate technological defences from everyday work practices, generating severe difficulties when attempting to assess or mitigate authentic organisational risks on the ground. This structural mismatch has reached a flashpoint in modern enterprises. As organisations rapidly scale cutting-edge technologies, the failure to integrate human governance has resulted in a massive, systemic AI oversight gap. The contemporary race for immediate corporate utility outpaces structural security architecture, transforming a long-standing communication mismatch into an enterprise-wide governance crisis. This shift confirms that when designing and securing systems at an industrial scale, the primary challenges cease to be technical artefacts and instead become entirely about human configuration and organisational behaviour [49].

To address this governance crisis, the primary aim of this paper is to evaluate the systemic, structural misfits between rigid, hard-systems information security management (ISM) standards and the fluid operational realities of real-world Human Activity Systems. Rather than treating non-compliance as a baseline human failure, our purpose is to demonstrate how top-down, non-contextual technical controls actively induce a behavioural backlash, such as the rapid proliferation of unmanaged *'Shadow AI'* workarounds. By synthesising multi-year empirical data with interpretive information systems theory, this study aims to dismantle the illusion of check-box compliance. Ultimately, we propose a holistic, socio-technical framework designed to reconcile information security with daily workflows, transforming front-line users from vulnerabilities into active co-designers of organisational resilience.

The remainder of this paper is structured as follows. Section 2 outlines the theoretical framework, contrasting the data processing paradigm with human activity systems. Sections 3 through 6 analyse industry standards, data classification failures, patching deficiencies, and the commercialisation of vulnerabilities. Section 7 presents empirical evidence of the policy-practice disconnect, while Section 8 discusses the resulting behavioural backlash and user workarounds. Finally, Section 9 proposes a holistic, socio-technical framework to reconcile security controls with legitimate human workflows.

2. Theoretical Framework: Shifting Paradigms from Data Processing to Human Activity Systems

To understand why purely technical cybersecurity interventions fail, we must examine the underlying information systems paradigms that guide design choices. Historically, the IS discipline has been influenced by two competing paradigms:

- **The Data Processing Paradigm (Hard Systems Thinking):** This approach focuses primarily on engineering effective IT artefacts. Rooted in hard systems thinking, it assumes that systems exist objectively in the real world and can be fully modelled, optimised, and engineered toward static, predefined objectives. Under this paradigm, end-users are rarely integrated into the design or development process. Instead, implementation forces the organisation to adapt through top-down mandates, rigid procedures, and compliance training. When technical security controls are engineered using this hard systems ethos, a severe misfit occurs between system design and actual working practices, driving the high failure rate of traditional security initiatives.
- The Human Activity Systems Paradigm (Socio-Technical Thinking): Conversely, viewing an IS as a Human Activity System shifts the focus to the intricate interdependencies among human actors, cultural structures, and technical components within an evolving organisational environment. This perspective requires moving from rigid management or engineering practices towards a holistic socio-technical systems approach, ensuring that technical defences are systematically co-designed with the organisational processes and human cultures they are meant to safeguard [9, 36, 37]. As Alter [3] notes, "the fact that transportation systems use vehicles does not necessarily imply that vehicles are the core subject matter for the field of transportation studies; similarly, voting procedures are not required to be the core subject matter of studies of democracy." By extension, computers and software are not the core subject matter of information systems or cybersecurity. Instead, an information system must be understood as a social process in which data is conceptualised, interpreted, and utilised by human actors engaged in purposeful real-world action [10, 19]. When conceptualised as a human-organised activity via Soft Systems approaches, security development ceases to be a mere engineering task. Instead, it becomes an emergent learning process rooted in exploring, understanding, and adapting to contextual human dependencies.

This paradigm shift highlights a fundamental ontological critique within information systems theory, which warns that traditional frameworks fail because they treat data and knowledge as static objects ('nouns') to be controlled, rather than recognising them as human processes ('verbs') executed by organisational actors [10, 13, 37]. This conceptual shift directly parallels the transition in safety science from a 'Safety-I' orientation, which focuses on enforcing rigid compliance to eliminate human error, toward a resilient 'Safety-II' paradigm, which recognises that system security is dynamically maintained by the ability of human actors to adapt to variable operational realities [28]. Work System Theory (WST) offers a vital analytical lens to

bridge this paradigm gap. As Sadok, Alter, and Bednar [42] demonstrate through WST, corporate security policies are frequently disconnected from actual work practices because security is treated as an isolated technological overlay rather than an active component of daily workplace routines.

When technical infrastructure is designed in a functional vacuum, security mechanisms lose operational relevance to the human actors executing the system. Ignoring these localised realities of human activity forces users to adopt volitional workarounds to accomplish their core duties. Consequently, the system falls victim to a fundamental socio-technical irony where the implementation of security mechanisms directly creates organisational insecurity by rendering standard workflows unworkable [3, 6]. This behavioural friction highlights the enduring relevance of foundational socio-technical theory, which asserts that managing complex and volatile organisational situations requires a continuous restructuring of work systems to align technical rules with human problem-solving capacity [35, 36, 42]. In the contemporary digital workplace, this behavioural friction manifests acutely as the "Shadow AI" phenomenon, where employees deliberately adopt unmanaged generative AI tools as an adaptive work-system bypass to maintain productivity in the face of restrictive technical controls.

3. Industry Standards and the Traditional Security Management Process

To operationalise information security within organisational structures, industry practice relies heavily on formalised frameworks, most notably the ISO/IEC 27000 family [30]. Originating from the British Standard BS7799, this international suite of standards provides a structural benchmark for organisational security. At its core is ISO/IEC 27001, the international Information Security Management System (ISMS) standard, originally published in 2005 and subsequently updated in 2013 and 2022 (ISO/IEC, 2022) [30].

ISO/IEC 27001 offers best-practice recommendations for initiating, implementing, and maintaining an ISMS. Crucially, the standard dictates that an ISMS must be tailored to meet the specific needs of the organisation. Rather than a purely technical deployment, an ISMS is formally defined as a core component of the overall management system, leveraging a business risk approach to establish, execute, monitor, and improve information security through organisational structures, policies, practices, and resources. The fundamental objective of an ISMS is the preservation of three core principles:

- **Confidentiality:** Ensuring information is not disclosed to unauthorised individuals, entities, or processes.
- **Integrity:** Protecting the accuracy and completeness of information assets.
- **Availability:** Ensuring information is accessible and usable upon demand by an authorised entity.

In practice, a significant socio-technical difficulty arises here: achieving an optimal balance between these core principles is notoriously difficult. Enforcing extreme confidentiality through aggressive encryption and multi-factor authentication often restricts availability, disrupting the daily workflow of human operators. To navigate these tensions, traditional security

management relies on a structured, mathematical risk analysis process. This workflow acts as the key input for security policy development and follows a linear trajectory: identification of vulnerabilities and threats, risk estimation (*Risk = Vulnerabilities x Threats*), cost-benefit analysis, and risk treatment (*avoid, transfer, mitigate, accept or increase*).

However, treating risk as a purely calculable, static math equation is a fundamental error; true security and crisis management must instead be understood through organisational culture, simulation, and the human perception of threat environments [7, 13, 17]. This limitation highlights a foundational critique in information systems research, which establishes that mathematical risk analysis should not be treated as an objective engineering truth, but rather as an interpretive feasibility tool to understand organisational dynamics and human constraints [7, 42, 61].

As Siponen and Willison [47] demonstrate, mainstream information security management standards suffer from deep-seated conceptual and practical problems. They present ambiguous, overly rigid directives that treat risk as a static, calculable metric. They assume that human behaviour, organisational culture, and technical infrastructure can be fully mapped into a predictable equation, ignoring the emergent, unpredictable dynamics of Human Activity Systems [36, 37].

This critical limitation is increasingly recognised by international regulatory bodies. The legislative implementation of the NIS2 Directive has triggered a massive regional push for structural auditing, yet it reveals deep disparities in organisational maturity and a systemic struggle to translate top-down legal requirements into functional workplace capabilities (ENISA, 2024) [23]. As documented in the ENISA Threat Landscape 2025 report [24], mapping modern enterprise risk effectively demands a distinct departure from rigid, checklist-driven compliance, advocating instead for a "*threat-centric approach*" and deeper "*contextual analysis*". Evaluating real-world cyber incidents across Europe establishes that threats cannot be treated as isolated mathematical components; they are dynamic, variable phenomena that can only be understood when evaluated against the unique operational and organisational context of the target entity.

This operational disconnect is compounded by systemic flaws in how organisational compliance is studied at an academic level. A comprehensive systematic literature review conducted by Gerdin, Grönlund, and Kolkowska [26] reveals conceptual inconsistencies in variable definitions and measurement items within Information Security Policy (ISP) compliance research. The study highlights that mainstream security research routinely relies on fragmented, poorly defined metrics that fail to capture the multi-dimensional reality of human behaviour in the workplace. This lack of conceptual standardisation means that the industry's baseline understandings of compliance and non-compliance are often built on superficial indicators. It explains why organisations remain trapped in an illusion of compliance: the metrics used to evaluate security adherence focus heavily on static, self-reported checkboxes while completely ignoring the fluid, fast-paced work system dynamics where actual security violations occur [42].

This omission of the human element is empirically validated by Ewoh, Vartiainen, and Mantere [25]. In a comprehensive scoping review evaluating cybersecurity frameworks within highly complex healthcare environments, the authors highlight a profound structural deficit: prominent industry-standard frameworks (such as NIST, ISO/IEC, COBIT, and IT-CMF) fail to fully satisfy the security requirements of a socio-technical system's social dimension. By leaving

the social layer fundamentally incomplete, these standards encourage an engineering-focused vacuum that separates a system's technical rules from its real-world human environment [25, 35, 36]. This critical deficit is further illuminated when evaluating state-sponsored hybrid warfare, where traditional compliance benchmarks fail to anticipate multi-vector operational disruptions, necessitating threat modelling to quantify and systematically mitigate elevated risk vectors across digital governance infrastructure [53].

4. The Critical Failure Point: Data Classification and the Growth of Dark Data

A foundational component of any Information Security Management System (ISMS) is data classification. In theory, classification categorises information assets based on their sensitivity and business value to ensure proportional protection. Traditional frameworks and modern automated labelling tools typically enforce a rigid taxonomy ranging from highly restricted to public tiers. To operationalise these schemas, organisations must maintain an exhaustive inventory of data assets and assign explicit structural responsibilities for data ownership [7].

While straightforward in theory, data classification remains a profoundly overlooked activity among security professionals. Organisations struggle with execution because standard frameworks provide ambiguous, non-user-friendly methods for everyday context. This operational stagnation occurs because traditional compliance frameworks treat data assets as passive commodities to be catalogued in an administrative vacuum, ignoring the reality that information value and sensitivity are continuously constructed through the daily actions and routines of human operators [37]. This systemic deficit was highlighted a decade ago when the Global Databerg Report revealed that a mere 48% of organisational information was actively classified, leaving 52% as "*dark data*", unstructured information whose risk profile remains completely invisible [55]. As Bergström, Karlsson, and Åhlfeldt [14] and Mumford [36] emphasise, unclassified data creates operational chaos: employees are routinely denied access to data required for daily tasks or, conversely, inadvertently inherit permissions to highly sensitive assets.

In the contemporary computing landscape, this legacy governance failure has mutated into an unprecedented socio-technical crisis. The structural inability to catalogue enterprise data has directly fueled the rapid proliferation of unmanaged artificial intelligence tools. According to the IBM Cost of a Data Breach Report 2025 [29], a staggering 63% of organisations lack any formalised AI governance policies to track or restrict the explosive growth of "*Shadow AI*", the unauthorised operational use of public AI tools by employees to fulfil daily duties. Furthermore, 97% of organisations experiencing an AI-related security incident actively lacked proper AI access controls.

This macro-level vulnerability has fundamentally reoriented executive anxiety. Corporate leaders' primary concerns have inverted from external adversarial capabilities to internal, inadvertent data exposure [58]. The WEF data demonstrates that data leaks associated with commercial generative AI use (34%) now heavily outweigh executive fears regarding advanced offensive AI exploits (29%) [58]. This empirical shift validates the Human Activity Systems paradigm: the dominant modern risk vector is not a malicious external code exploit, but the fluid, daily routines of well-meaning human users pumping unclassified enterprise data into public LLM models to maintain operational velocity [3, 10, 42]. This behavioural dynamic

perfectly illustrates Mumford's [36] critique of *'dangerous decisions*,' wherein executives implement restrictive technical boundaries under the assumption that human workflows will naturally conform to digital cages. A classic manifestation of this friction is observed when an enterprise locks down file-sharing capabilities to protect IP; rather than ceasing collaboration, well-meaning employees simply migrate corporate data to personal cloud systems or unmanaged Shadow AI tools to bypass the administrative lag, creating an unmonitored risk environment that completely breaks corporate perimeter vision. Confronting this shift requires discarding traditional static filters in favour of threat-informed defensive models that map emergent generative AI vulnerabilities and system behaviours into collaborative mitigation frameworks [18, 31].

5. The Industrial Scale of Code Complexity and the Myth of Patching

The traditional engineering calculation of risk assumes that vulnerabilities can be isolated and comprehensively patched. However, a socio-technical analysis reveals that modern information systems suffer from an industrial-scale accumulation of flaws driven by software complexity. In the software development industry, code contains bugs, with averages ranging between 15 and 50 errors per 1,000 lines of code. This defect rate scales exponentially as technical artefacts are embedded into cyber-physical infrastructure. For example, a modern commercial aeroplane (like the Boeing 737) relies on millions of lines of code, while a consumer vehicle such as the Ford F-150 truck contains an astonishing 150 million lines of code. Within such hyper-complex systems, vulnerabilities are not anomalies; they are statistical inevitabilities. This exposure is compounded as critical infrastructure environments become increasingly digitised and interconnected, turning legacy systems into highly vulnerable attack surfaces that resist traditional perimeter security controls [50].

This upward trajectory of systemic exposure is a permanent, structural reality of the enterprise software landscape. Looking at continuous long-term tracking by the annual BeyondTrust Microsoft Vulnerabilities Report series [15], total documented vulnerabilities consistently hold near record highs, with critical flaws frequently doubling year-over-year. This staggering volume creates an insurmountable "*vulnerability debt*" for organisations, weaponised by a booming dark web marketplace where nearly 50 new Common Vulnerabilities and Exposures (CVEs) are published daily.

The empirical reality of this debt is laid bare by Positive Technologies' [39] large-scale automated network perimeter assessments across 3,514 corporate hosts. Their findings revealed that high-risk vulnerabilities are present on the external network resources of 84% of companies, and 50% of these flaws could be eliminated simply by installing software updates. Yet, organisations globally fail to maintain basic patch currency, a failure driven by a severe socio-technical paradox: deploying a patch requires taking critical systems offline, which directly threatens system availability and disrupts legitimate human work [8, 9, 28].

The operational reality of this technical debt has reached a structural turning point. While legacy data traditionally blamed human negligence or stolen passwords as the primary vector for system intrusion, the Verizon 2026 Data Breach Investigations Report (DBIR) [56] reveals that 31% of breaches now start by exploiting software vulnerabilities. Systemic software flaws have officially surpassed stolen credentials as the leading initial entry point for threat actors.

The failure of this endless technical patching race highlights the need for a shift in strategy. Telemetry indices reveal that "*Elevation of Privilege*" (EoP) remains the number 1 vulnerability category, accounting for roughly 40% of all reported flaws [15]. Strikingly, the data proves that simply removing local administrative rights from users successfully mitigates up to 75% of all critical vulnerabilities [15]. This single procedural modification of user privileges delivers a higher security return than hundreds of complex technical software patches, proving that the solution to technical vulnerability accumulation lies within the social and organisational domain [36, 37].

6. The Commercialisation of Vulnerabilities and Ontological Reality of Risk

As organisations realise that technical patching cycles cannot keep pace with software complexity, they are increasingly turning to crowdsourced human intelligence through Security Bug Bounty Programs to identify these vulnerabilities before adversaries do. Platforms like HackerOne connect organisations with a global ecosystem of over 830,000 registered security researchers, converting external human capital into a critical defensive resource [60]. This crowd-powered model has transformed threat discovery into a highly commercialised industry, with hackers earning over USD 230 million on the platform [60]. Microsoft awarded USD 13.7 million in bounties over a single year, while Google paid out USD 3.1 million for Chrome vulnerability reports. In response to rapid infrastructure changes, this human threat landscape has accelerated: the HackerOne platform recorded a 210% increase in AI-specific vulnerability reports in a single year [60], proving that human adversaries adapt to new technological surfaces far faster than traditional defence models predict.

While the bug bounty economy highlights a highly sophisticated, financially motivated ecosystem of human actors, traditional information security management defines a threat broadly as a *'potential cause of an unwanted incident*,' neatly divided into Natural, Environmental, or Human sources. A socio-technical lens reveals that modern security risks possess ontological characteristics that resist these rigid, static engineering categorisations. Confronting this hyper-complex ecosystem requires adopting critical systemic thinking as an interpretive foundation, recognising that threat environments are not objective external constants but are fluid phenomena continuously shaped by the shifting contexts and bounded observations of the human actors investigating them [10, 13]. This structural uncertainty manifests across several core socio-technical dimensions:

- **Uncertainty and Invisible Latency:** Attacks are highly stealthy; full visibility is frequently achieved only after an exploit chain has reached completion. This systemic blindness is underscored by recent industry data showing that companies require an average lifecycle of 245 days to identify and contain a single data breach [29].
- **Socio-Technical Complexity:** Heterogeneous, geographically distributed information systems allow remote adversaries to execute attacks from immense distances, making definitive hacker attribution exceptionally difficult. Human adversaries are inherently creative, bypassing technical perimeters through social engineering and business-logic exploitation. The ENISA Threat Landscape 2025 [24] report reveals that threat groups no longer operate in isolated silos; instead, diverse

adversary collectives collaborate, reuse malicious tools, and introduce hybrid, convergent attack models. This evolution underscores a broader shift where cyber exploits are no longer mere localised technical breaches but are actively deployed as strategic instruments of modern conflict targeting vital civilian infrastructure to achieve macro-political objectives [2].

- **Unpredictability and Reactive Defences:** Traditional security technologies, such as signature-based antivirus software, firewalls, and basic intrusion detection systems (IDS), are inherently reactive, engineered to detect only known attack vectors. Consequently, they offer minimal protection against zero-day exploits or novel threat mutations. Threat actors leverage generative AI to bolster 15 distinct attack techniques [56]. Furthermore, the threat landscape shifts across organisational surfaces: the 2026 Verizon report captures an aggressive expansion into mobile spaces, revealing that mobile devices suffer from a 40% higher phishing click rate than traditional email communication [56]. This rapid exploitation of mobile channels relies on highly agile adversarial patterns, where cybercriminals deliberately bypass detection by purchasing short-lived, newly registered domains that impersonate trusted brands to host malicious infrastructure, surviving for an average of only 8.6 days before abandonment [4]. This constant cat-and-mouse dynamic proves that security risks are socio-technical anomalies that cannot be engineered out of existence via static tools. As Mumford [36] asserts, treating volatile risk environments as static data-processing problems ensures defences remain purely reactive. True security choices are inherently socio-technical decisions; if a tool diminishes an operator's capability to react fluidly to customer or operational demand, the social system will naturally subvert the defence model to stabilise its immediate environment [35, 36, 45].

This mutation of threat surfaces underscores how the integration of machine learning-based artificial intelligence fundamentally introduces parallel channels of vulnerability, complicating system defences across malware and phishing detection vectors [21]. The WEF Global Cybersecurity Outlook 2026 survey [58] corroborates this reality, revealing that 87% of global cybersecurity and business leaders identify AI-related vulnerabilities as the fastest-growing cyber risk facing modern enterprises. Threats operate within a socio-technical ecosystem where the line between defensive security researchers and malicious actors is mediated by financial incentives, market economics, and organisational accessibility. This means that technology itself possesses a limited scope when countering complex behaviours like cyber-enabled industrial espionage and insider threats, which can only be mitigated by bridging the design of security solutions with the active integration of an organisational culture [44]. Ultimately, confronting this hyper-complex reality requires moving away from reductionist engineering templates toward holistic problem-solving models that recognise technical risk choices as inherently dangerous organisational decisions affecting human systems [36, 37].

7. Empirical Evidence of the Governance and Policy-Practice Disconnect

The theoretical misfits of the hard systems paradigm and the structural friction of traditional risk models are reflected in enterprise governance data. Historically, the Cyber Security

Breaches Survey 2021 [54] exposed a profound failure to operationalise socio-technical risk management, noting that only 34% of UK businesses carried out formal risk assessments, and a mere 33% maintained documented cybersecurity policies [54]. Furthermore, responsibility was highly fractured and de-professionalised: in micro and small businesses, security was typically assumed by general business owners (16%) or directors outside of IT (29%), with just 10% employing a dedicated IT professional in a security role.

Contemporary empirical telemetry reveals that this policy-to-practice disconnect remains stalled. According to the official Cyber Security Breaches Survey 2026, despite years of escalating technical threats, only 25% of UK businesses and 19% of charities maintain a formal, documented incident response plan [51]. This governance stagnation (e.g., only 25% having incident plans) is precisely why organisations are entirely unequipped to handle the swift adoption of emergent technologies like Shadow AI. The massive gap between casual assignment and structured, documented processes remains unchanged year-on-year, illustrating that companies treat incident readiness as an ad hoc, reactive human burden rather than a core system capability [7]. This stagnation occurs because traditional enterprise training models separate manual exercise compilation from dynamic threat developments, highlighting a requirement to integrate automated threat forecasting directly into the cybersecurity exercise generation lifecycle [59]. This structural stagnation directly contradicts the strategic requirements of modern risk environments, where true resilience demands an 'incident-centred' security model that balances technical prevention with formalised organisational response capabilities [8]. This governance failure is compounded by acute supply-chain blindness: just 15% of UK businesses review the cybersecurity risks posed by their immediate suppliers, a metric that drops to 12% among micro-businesses.

This localised structural exclusion is thoroughly detailed in empirical research. Sadok, Alter, and Bednar [42] conducted a firm-level study across 39 UK firms, analysing 187 employees handling sensitive data. Their findings revealed that front-line operational staff are rarely involved in security risk assessments or policy development. This deliberate exclusion reduces policy legitimacy, causing employees to view corporate security as a detached, "*illusory activity*" that is unaligned with their actual workplace realities [35, 36, 42, 62].

This baseline disconnect cannot be addressed with a generic, one-size-fits-all framework, as doing so fuels a dangerous macroeconomic condition that the WEF Global Cybersecurity Outlook 2026 defines as "*cyber inequity*" [58]. The report warns of a rapidly widening capability gap separating highly resilient, heavily resourced global organisations from smaller, underfunded enterprises that lack structural cybersecurity maturity. While 64% of mature organisations successfully scale their security postures to assess AI tools before deployment, smaller entities remain left behind. This macroeconomic imbalance reinforces Renaud's [40] assertion that smaller businesses find mainstream, rigid security advice unworkable. Because standard security guidelines are heavily optimised for large enterprises with mature IT budgets, small business owners find the advice overly technical, complex, and resource-heavy. Consequently, they reject formal frameworks and absorb the security function into non-technical roles, generating deep procedural vulnerabilities that trigger an inevitable behavioural backlash. This vulnerability is heavily exacerbated by regional isolation; large-scale cross-border data proves that localised, bilateral security formats are structurally outpaced by modern threat surfaces [34].

8. Discussion: The Illusion of Compliance and the Behavioural Backlash

The mere existence of a security policy does not guarantee its effective implementation or its relevance from an operational perspective. Writing a policy on paper satisfies a compliance checkbox, but it frequently introduces friction within real-world human activity systems. When organisations rely on top-down, hard-systems engineering to impose rigid security controls, they disrupt daily human workflows. Rather than securing the organisation, this systemic mismatch triggers a behavioural backlash where users intentionally bypass policies to maintain operational efficiency.

When security architecture fails to match the real-world velocity of business transactions, employees prioritise productivity over compliance. A field study captured this from an organisational perspective [31]:

"*The new access rules mean that we have to wait for approvals through the chain of command. Unfortunately, when one is with a client, they have to take decisions instantaneously. In such instances, we simply do not use the system…. now I know that this can have possible security and compliance ramifications, but at the same time I have a job to do and services to render.*"

This conflict between rigid technical protocols and urgent real-world duties manifests acutely in high-stakes environments [36, 37]. This tension has been documented in clinical settings, demonstrating that when technical access controls block a practitioner from treating an acute patient, the human actor will subvert security boundaries to preserve human life [32]. This operational friction is equally pronounced in frontline public safety domains, where enforcing rigid, non-contextual security controls during high-velocity field tasks, *such as digital device triage*, forces personnel to bypass technical protocols to achieve immediate operational outcomes, proving that ignoring usability principles directly compromises security integrity [57].

Henshaw and Mhajne (2025) [27] observe that top-down security architectures introduce institutional discipline that prompts employee resistance and subversion in online spaces. This operational friction triggers a classic socio-technical paradox where the security menace itself actively creates insecurity; when technical controls block an operator's primary job function, the human activity system generates adaptive workarounds to preserve productivity [6]. This proves that security models designed solely to police behaviour rather than support operational workflows trigger non-malicious compliance failures. When technical controls block an operator's primary job function, the human activity system generates adaptive workarounds, proving that security models designed solely to police behaviour rather than support operational workflows trigger non-malicious compliance failures. This compliance failure is heavily mediated by the level of psychological safety within work teams; when punitive controls eliminate the safety required to admit operational friction or technical limitations, well-meaning employees choose to obscure their routines, deploying unmanaged workarounds in an environment of hidden risk rather than engaging in open learning behaviours [22]. This tension is exacerbated by the broader datafication of the contemporary workplace, where invasive AI-driven monitoring and data collection fuel deep-seated privacy concerns and work-life conflict among personnel, directly undermining employee engagement and structural organisational [4, 52, 54].

This resistance is driven by a documented psychological threshold in policy legitimacy; empirical data confirms that while heightened threat awareness increases an individual's desire for structural security, the enforcement of overly intrusive or rigid policies actively erodes user support and destroys compliance motivations [6, 31, 48]. This widespread rejection of generic compliance programs points to a structural flaw in traditional education models: the information security domain routinely treats the workforce as a homogeneous entity. Security awareness methods are often applied without considering the specific psychological traits of the targeted audience.

This instructional failure is compounded by the core limitation of corporate knowledge transfer frameworks, which routinely mistake simple information delivery for authentic human understanding, failing to recognise that managing volatile threat environments requires complex methods of inquiry rather than standardised, top-down instruction [11, 12]. By returning to Nissen's (2012) [37] ontological critique, we can see that this failure occurs because static compliance policies treat security as a rigid *'noun'*, a frozen set of rules to be distributed and checked off. In doing so, they fail to protect a dynamic workplace where actual risk is an evolving, fast-paced 'verb' executed during daily operations. When an organisation forces a *'noun-based'* compliance template onto *'verb-based'* human activity, it creates an operational vacuum. Well-meaning employees are left with no choice but to deploy volitional workarounds [3, 6], transforming security from a protective shield into an administrative barrier that must be bypassed to keep the business running.

This instructional failure is compounded by the core limitation of corporate knowledge transfer frameworks, which routinely rely on conceptually inconsistent theories that mistake simple information delivery for authentic human understanding. To bridge this user-designer gap, modern information security management must incorporate individual behavioural and cognitive differences into system defence. It is possible to address this deficit by systematically mapping distinct personality types using the DISC model, adapting to specific learning styles and social engineering vulnerabilities [16]. Findings demonstrate that a uniform training approach is structurally non-viable [16]; instead, optimal information security awareness requires matching an individual's dominant psychological profile (dominant, influencing, steady, or compliant) with tailored delivery methods and message framing. By aligning training with the diverse learning preferences and psychological baselines of the workforce, organisations can transition away from coercive mandates toward a participatory learning architecture where secure behaviours are sustainable.

The structural cost of this paradigm failure is laid bare by contemporary national statistics. The Cyber Security Breaches Survey 2026 reveals that 43% of UK businesses experienced an active cyber breach or attack over the prior 12 months (DSIT, 2026) [51]. Furthermore, ransomware is now involved in 48% of all analysed global data breaches [56]. Following a security incident, the vast majority of organisations (61%) react by introducing even more restrictive internal policies or generic awareness training [9, 51]. However, empirical evaluation confirms that standard, passive Security Education, Training, and Awareness (SETA) solutions remain fundamentally ineffective at altering long-term human risk baselines, highlighting a critical requirement for a shift toward interactive, experiential learning modalities [41]. Real professional as well as organisational learning is a continuous sense-making process [19]. By shifting security training from a passive compliance broadcast into an open arena for collective reflection, organisations allow users to explicitly negotiate the boundaries between technical

rules and operational demands. This converts security from an externalised technical overlay into an intrinsic, shared understanding of work system resilience. This counterproductive practice represents a classic failure of 'single-loop learning,' where an enterprise attempts to fix an anomaly by amplifying the exact defensive rules that caused the friction in the first place, rather than engaging in 'double-loop learning' to fundamentally interrogate the underlying assumptions of their security design [5, 10].

Contemporary risk management maintains an excessive focus on data system security while ignoring the operational organisational context [43]. Ineffective operational and communication design does not stop human work [25]; instead, it strips front-line staff of their ability to maintain agile workflows, rendering the organisation fragile to threat exploits. Because these educational and technical measures remain detached from the contextual pressures of daily employee workloads, they result in operational friction rather than genuine security, failing to halt the cycle of human-related security incidents.

9. Conclusion: Putting It All Together via a Holistic Socio-Technical Approach

To resolve the compounding crises of dark data, shadow AI, unworkable security policies, and human workarounds, the cybersecurity domain must move away from its narrow, technology-centred view. An exclusive emphasis on technical infrastructure introduces fundamental flaws into both the design and implementation of protective solutions. Security procedures imposed through a strictly top-down lens are not only highly vulnerable to systemic misuse, but they actively operate as structural barriers to legitimate daily work.

To mitigate these non-malicious compliance failures, organisations must target the underlying "*it is not my job*" mindset [42]. Security can no longer be handled as a detached, external administrative mandate; it must become a co-designed, participatory, and embedded workplace value that recognises the reciprocal relationships between human actors and technical components.

Bridging this communications and sense-making gap requires a holistic, socio-technical approach to information security management organised around three fundamental operational pillars:

- **Participatory Co-Design over Top-Down Dictates:** Front-line professionals possessing rich operational knowledge must be integrated directly into risk analysis and policy formulation [46]. This collaborative approach operationalises a 'Safety-II' philosophy, transforming security controls from restrictive policies designed to constrain employees into adaptive mechanisms that support everyday legitimate work [28]. Security policies co-authored with the users who execute them ensure controls support, rather than sabotage, daily business productivity. This inclusive methodology operationalises Cherns' [20, 35, 36] design principles, which dictate that those who populate and execute a system must be the central actors in its organic architectural formulation. This co-design phase explicitly targets two critical areas: technical security requirements and human job satisfaction [36]. If front-line operators are empowered to actively co-author security exceptions and protocol pathways, the technical rules

become extensions of their workflow rather than external barriers, eliminating the very operational friction that triggers the deployment of unmanaged workarounds

- **Dialogue and Collective Reflection:** Security training must evolve from a passive checklist exercise into an active engagement space. Engaging users through small-group workshops focused on local dialogue, peer participation, and collective reflection improves real-world security behaviours far more effectively than expert-led, passive awareness campaigns [1]. To operationalise this conversational layer, organisations must intentionally cultivate a team climate of psychological safety, ensuring that front-line workers feel secure taking interpersonal risks, voicing systemic vulnerabilities, and participating in collective reflection without fear of administrative penalties [10, 22, 35]. This requires actively facilitating constructive dialogue to unlock hidden operational competencies and dismantling organisational defence mechanisms that traditionally isolate technical design from human realities [10]. This shift can be operationalised by abandoning flat text templates in favour of immersive, multiuser simulations and virtual environments that force active human coping and collaborative threat mitigation [41].
- **Contextual Analysis and Organisational Resilience:** All protective measures must be explicitly tied to local operational context and business needs [3]. Organisations must transition away from purely preventative, artefact-heavy paradigms toward an incident-centred security strategy that prioritises cross-functional response readiness alongside technical defences [8]. Industry data confirms that while technical automation can yield up to USD 1.9 million in data breach cost savings, these technologies are only optimised when anchored by broader organisational resilience [29]. This requires regular cross-functional crisis simulations and the continuous human testing of incident response plans.

Ultimately, genuine security cannot be achieved by enforcing compliance with sterile, off-the-shelf templates. Only by designing security systems with and for the human activity systems they protect can modern enterprises eliminate the friction that drives unmanaged workarounds like Shadow AI, achieving a sustainable, resilient, and authentic security posture.

Declaration on Generative AI

During the preparation of this manuscript, the author utilised Google Gemini (Gemini 1.5 Pro) to improve the readability, narrative structure, and thematic cohesion of the text. The author reviewed, edited, and verified all outputs generated by the AI assistant and assumes full accountability for the accuracy, originality, and integrity of the final text and its references.

References

[1] Albrechtsen, E. and Hovden, J. (2010), “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study”, *Computers and Security*, Vol. 29 No. 4, pp. 432-445.

[2] Aljohani, T. M. (2024), "Cyberattacks on energy infrastructures as modern war weapons – Part I: Analysis and motives," IEEE Technology and Society Magazine, Vol. 43 No. 1, pp. 59–69.

[3] Alter, S. (2003), "Sidestepping the IT artifact scrambles: The work system method for analyzing systems, cases, and concepts," *Communications of the Association for Information Systems*, Vol. 12 No. 1, p. 36.
[4] Agarwal, S. and Vasek, M. (2026), "Examining newly registered phishing domains at scale," Journal of Cybersecurity, Vol. 12 No. 1, article ID: tyag020. https://doi.org/10.1093/cybsec/tyag020
[5] Argyris, C. and Schön, D. A. (1978), Organizational Learning: A Theory of Action Perspective, Addison-Wesley, Reading, MA.
[6] Balozian, P. and Leidner, D. (2016), "IS security menace: when security creates insecurity", *Proceedings of Thirty Seventh International Conference on Information Systems*, Association for Information Systems, Dublin, Ireland.
[7] Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems, 1(2), 121-130. https://doi.org/10.1057/ejis.1991.20
[8] Baskerville, R., Spagnoletti, P. and Kim, J. (2014), "Incident-centered information security: Managing a strategic balance between prevention and response," Information & Management, Vol. 51 No. 1, pp. 138-151.
[9] Baxter, G., Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering, Interacting with Computers, Volume 23, Issue 1, January 2011, Pages 4–17, https://doi.org/10.1016/j.intcom.2010.07.003
[10] Bednar, P. (2000). A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis. Informing Science: the International Journal of An Emerging Transdiscipline, 3(3), 145-156. http://inform.nu/Articles/Vol3/v3n3p145-156.pdf
[11] Bednar, P., Anderson, D., & Welch, C. (2005). Knowledge Creation and Sharing – Complex Methods of Inquiry and Inconsistent Theory. In D. Remenyi (Ed.), Proceedings of the European Conference on Knowledge Management (ECKM). (pp. 59-66). Academic Conferences.
[12] Bednar, P., & Katos, V. (2009). Addressing the human factor in information systems security. In MCIS2009: 4th Mediterranean Conference on Information Systems (pp. 900-912). Athens University of Economics and Business.
[13] Bednar, P. & Welch, C. (2012). Critical systemic thinking as a foundation for information systems research practice. Journal of Information, Communication and Ethics in Society (2012) 10 (3): 144–155. https://doi.org/10.1108/14779961211261058
[14] Bergström, E., Karlsson, F. and Åhlfeldt, R.-M. (2021), "Developing an information classification method", *Information and Computer Security*, Vol. 29 No. 2, pp. 209–239.
[15] BeyondTrust (2026), *The Microsoft Vulnerabilities Report*, Annual Whitepaper Research Series (13th Ed), BeyondTrust Resource Center.
[16] Bjorn, S., Jashari, V., Kolkowska, E., & Gao, S. (2026), "Developing and testing a framework for matching distinct personality types with information security awareness methods," *Information and Computer Security*, Vol. 34 No. 2, pp. 246–272.
[17] Borodzicz, E. P. (2005). Risk, crisis and security management. Wiley.
[18] Center for Threat-Informed Defense (2025), 2024 Impact Report: Celebrating Five Years, MITRE Corporation, Center for Threat-Informed Defense R&D Series. https://ctid.mitre.org/resources/2024-impact-report/2024%20Impact%20Report%20Center%20for%20Threat-Informed%20Defense.pdf

[19] Checkland, P., & Holwell, S. (1998). Information, systems and information systems: Making sense of the field. John Wiley & Sons.
[20] Cherns, A. (1976), "The principles of socio-technical design," Human Relations, Vol. 29 No. 8, pp. 783–792. Aug. 1976, doi: 10.1177/001872677602900806.
[21] Czaja, P., Gdowski, B., Niemiec, M., Mees, W., Stoianov, N., Votis, K., Kharchenko, V., Katos, V., Merialdo, M., (2025). Cybersecurity challenges and opportunities of machine learning-based artificial intelligence. Neural Computing and Applications, 37 (33), 27931-27956.
[22] Edmondson, A. (1999). 'Psychological safety and learning behavior in work teams', Admin. Sci. Q., vol. 44, no. 2, pp. 350–383, Jun. 1999, doi: 10.2307/2666999.
[23] European Union Agency for Cybersecurity (ENISA) (2024), 2024 Report on the State of the Cybersecurity in the Union, European Union Cybersecurity Report Series, ENISA Publications. https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union
[24] European Union Agency for Cybersecurity (ENISA) (2025), *ENISA Threat Landscape 2025*, European Union Cybersecurity Report Series, Version 1.2 (Revised January 2026), ENISA Publications.
[25] Ewoh, P. Vartiainen, T. & Mantere, T. (2025). Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review. *Journal of Medical Internet Research*, 27.
[26] Gerdin, M., Grönlund, Å., & Kolkowska, E. (2025), "Conceptual inconsistencies in variable definitions and measurement items within ISP non-/compliance research: A systematic literature review," *Computers & Security*, Vol. 152. article ID: 104365.
[27] Henshaw, A., & Mhajne, A. (2025), "Beyond the Basics: Critical Perspectives on Cybersecurity in International Relations," *Global Studies Quarterly*, Vol. 5 No. 3. article ID: ksaf067.
[28] Hollnagel, E. (2014), Safety-I and Safety-II: The Past and Future of Safety Management, Ashgate Publishing, Farnham.
[29] IBM Security and Ponemon Institute (2025), *Cost of a Data Breach Report 2025*, IBM Corporation, IBM Reports Portal.
[30] ISO/IEC (2022), ISO/IEC 27001:2022: Information security, cybersecurity and privacy International Organization for Standardization / International Electrotechnical
[31] Kolkowska, E. and Dhillon, G. (2013), "Organizational power and information security struggles," *European Journal of Information Systems*, Vol. 22 No. 1, pp. 108-124.
[32] Koppel, R., Smith, S., Blythe, J. and Kothari, V. (2015), "Workarounds to computer access in healthcare organizations: you want my password or a dead patient?", *Studies in Health Technology and Informatics*, Vol. 280, pp. 211–220.
[33] Laudon, K. C., & Laudon, J. P. (2007), *Management Information Systems: Managing the Digital Firm*, 10th ed., Prentice Hall.
[34] Li, X. (2025), "Cybercrime prevention on the agenda of modern international relations," Foreign Affairs, Vol. 35 No. 3, pp. 115–127. https://doi.org/10.59214/2663-2675.35(3).2025.115
[35] Mumford, E. (1997). "Assisting Work Restructuring in Complex and Volatile Situations," in Developing Organizational Consultancy, J. E Neumann, K. Kellner, and A. Dawson-Shepherd (eds.). London: Routledge, 1997.

[36] Mumford, E. (1999). Dangerous decisions: Problem solving in tomorrow's world. Kluwer Academic/Plenum Publishers.
[37] Nissen, H.-E. (2012). What or whom do knowledge-managers manage? In J. G. Cegarra (Ed.), Proceedings of the 13th European Conference on Knowledge Management (pp. 839–847). Academic Conferences and Publishing International Limited.
[38] Oz, E. and Jones, A. (2008), *Management Information Systems*, 6th ed., Cengage Learning.
[39] Positive Technologies (2020), *Vulnerabilities on the Corporate Network Perimeter: Results of Automated Security Assessment,* Positive Technologies Research Report.
[40] Renaud, K. (2016), "How smaller businesses struggle with security advice*", Computer Fraud and Security*, Vol. 2016 No. 8, pp. 10-18.
[41] Sadeghi, M., Ghanbari, H., & Rossi, M. (2025). Designing a multiuser security education, training, and awareness (SETA) module using virtual reality (VR). In ECIS 2025 Proceedings (European Conference on Information Systems Proceedings). Association for Information Systems. https://aisel.aisnet.org/ecis2025/security/security/11
[42] Sadok, M., Alter, S. and Bednar, P. (2020), "It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs*", Information and Computer Security*, Vol. 28 No. 3, pp. 467–483.
[43] Sadok, M. and Bednar, P. (2015), "Understanding Security Practices Deficiencies: A Contextual Analysis", in Furnell, S. and Clarke, N. (Ed.), *Human Aspects of Information Security & Assurance*, HAISA 2015, Lesvos, Greece, July 1-3, pp. 151-160.
[44] Sadok, M., Welch, C., & Bednar, P. (2019). A socio-technical perspective to counter cyber-enabled industrial espionage. Security Journal, 33, 27-42 https://doi.org/10.1057/s41284-018-00198-2
[45] Sarker, S., Chatterjee, S., Xiao, X., Elbanna, A., The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance, MIS Quarterly 43 (2019) 695–720.
[46] Shedden, P., Smith, W., & Ahmad, A. (2011), "Information security risk assessment: Towards a business-focused methodology," *Proceedings of the 9th Australian Information Security Management Conference*, Edith Cowan University, Perth, Western Australia.
[47] Siponen, M. and Willison, R. (2009), "Information security management standards: Problems and solutions", *Information & Management*, Vol. 46, pp. 267-270.
[48] Snider, K. L. G., Shandler, R., Zandani, S. and Canetti, D. (2021), "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," Journal of Cybersecurity, Vol. 7 No. 1, article ID: tyab019.
[49] Sommerville, I. (2015). Designing software for a million users: It's not about the technology (Keynote). In Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS 2015) (CEUR-WS.org, Vol. 1374, pp. 1–4)
[50] Sontan, A. D. and Samuel, S. V. (2024), "Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review," Computer Science & IT Research Journal, Vol. 5 No. 3, pp. 576–593.
[51] UK Department for Science, Innovation and Technology (DSIT) (2026), *Cyber Security Breaches Survey 2025/2026*, Official National Statistics Report, GOV.UK Digital Collection.
[52] Teebken, M., Constantiou, I., & Tuunainen, V. K. (2025). Datafication at work: navigating AI, privacy concerns, and employee engagement. In ECIS 2025 Proceedings (European

Conference on Information Systems Proceedings). Association for Information Systems. https://aisel.aisnet.org/ecis2025/persdata/persdata/1

[53] Tovkun, Y., Semerenska, V. and Adamov, A. (2026), "An overview of cyber attacks on critical cyber-physical systems and government infrastructures," Security and Safety, Vol. 5, Article No. 2026002. https://doi.org/10.1051/sands/2026002

[54] UK Department for Digital, Culture, Media & Sport (2021), *Cyber Security Breaches Survey 2021*, National Statistics Report.

[55] Veritas Technologies (2016), *The Global Databerg Report: See What's Lurking in Your Data*, Veritas Strategy Brief.

[56] Verizon (2026), *2026 Data Breach Investigations Report (DBIR)*, 19th Edition, Global Security Analysis Series, Verizon Business Resources.

[57] Warner, M., Abreu, V. M. and O'Brien, C. (2026), "Police Officers Are Not the Enemy: Applying Usable Security Knowledge and Principles to Digital Device Triage in Policing," Proceedings of the Festschrift Symposium for Professor Angela Sasse, London, UK.

[58] World Economic Forum & Accenture (2026), *Global Cybersecurity Outlook 2026, Flagship Global Insight Report*, 5th Edition, World Economic Forum Centre for Cybersecurity, Geneva, World Economic Forum Publications.

[59] Zacharis, A., Katos, V., Patsakis, C., (2024). Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. International Journal of Information Security, 23 (4), 2691-2710.

[60] HackerOne. (2025). "The 9th annual hacker-powered security report: The rise of the bionic hacker," HackerOne Inc., San Francisco, CA, Tech. Rep., Oct. 2025. [Online]. Available: www.hackerone.com

[61] Bednar, P., Sadok, M. (2024). Information Security: Still Not My Job!. In: Agrifoglio, R., Lazazzara, A., Za, S. (eds) Navigating Digital Transformation. Lecture Notes in Information Systems and Organisation, vol 73. Springer, Cham. https://doi.org/10.1007/978-3-031-76970-2_5

[62] Sparrius, M., Sadok, M., Bednar, P. (2021). What Can We Learn from the Analysis of Information Security Policies? The Case of UK's Schools. IFIP Advances in Information and Communication Technology DOI: 10.1007/978-3-030-81111-2_7