The Hidden Costs of Disconnected IT

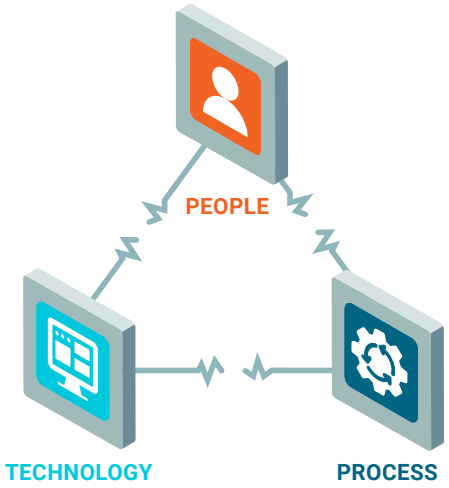
Why businesses must align people, processes, and technology to thrive

THE NEW REALITY OF BUSINESS DISRUPTION

Over the past five years, businesses have faced relentless waves of disruption—economic uncertainty, supply chain breakdowns, escalating cyber threats, and rapid shifts in how people work. The pace of technological change has only accelerated, forcing organizations to adapt in real time.

In response, many businesses have made incremental adjustments, implementing new tools, refining individual processes, or shifting workforce strategies. Yet, despite these efforts, inefficiencies persist. Systems remain fragmented, workflows lack adaptability, and employees struggle with misaligned processes that hinder productivity.

The problem isn't isolated failures—it's a disconnect between the parts and the whole. The challenge is clear: Unless businesses align their **people**, **processes**, and **technology** and take a system-thinking view of the organization, they risk further inefficiencies, disruptions, and stunted growth. Addressing these disconnects is critical to achieving sustainable operational resilience and efficiency.



THE FRAGMENTATION PROBLEM

Businesses rely on a growing number of tools, platforms, and systems to manage their operations. While these technologies are intended to improve visibility and efficiency, they often create the opposite effect—fragmentation. Instead of working seamlessly together, data and workflows become siloed, making it difficult to get a complete picture of performance, risk, and opportunity.

On average, organizations use 11 different monitoring tools,[1] yet research soon to be released by SolarWinds and ESG found that 52% still lack full-stack observability, leaving them missing critical performance issues. This disconnect is amplified by hybrid IT environments, where applications run across on-premises infrastructure, cloud platforms, and edge locations, each requiring its own specialized tools. As a result, businesses struggle to align their technology landscape, making cross-functional collaboration and decision-making more difficult.

On average, organizations use **11 different monitoring tools**.

When systems, teams, and workflows don't connect, businesses face significant operational challenges:

- **Frequent outages and downtime:** According to a 2022 report from the Uptime Institute, human error has caused nearly 40% of all major incidents over the previous three years.[2] Downtime can cost businesses anywhere from thousands

[1] "State of ITSM Report," SolarWinds. (Accessed February 2025).

[2] "2022 Outage Analysis Finds Downtime Costs and Consequences Worsening," Uptime Institute. (Published 2022, Accessed February 2025).

to millions of dollars per hour, with 44% of organizations reporting hourly losses exceeding $1 million.[3]

- **Slow incident resolution:** Disconnected telemetry and poor visibility extend the time it takes to diagnose and resolve issues, increasing Mean Time to Resolution (MTTR) and violating service-level agreements (SLAs).
- **Lost revenue and customer trust:** IT disruptions don't just impact productivity—they erode brand reputation. Customers expect seamless experiences, and repeated outages or inefficiencies reduce trust, leading to lost business and damaged long-term relationships.
- **Inefficient workflows and wasted effort:** Isolated teams using different tools and datasets leads to redundant work, slower decision-making, and missed opportunities.
- **Reactive rather than proactive management:** Without a unified, system-wide view, businesses spend more time addressing issues as they arise rather than proactively preventing them.

Instead of driving efficiency and control, disconnected systems force teams into a constant firefighting mode, limiting their ability to focus on innovation and strategic growth.

The key to overcoming these challenges isn't simply adopting more technology—it's ensuring that **people**, **processes** and **technology** work as a unified system rather than isolated parts. Without this alignment, businesses will continue to experience operational drag and struggle to keep pace with an increasingly complex landscape.

Downtime can cost businesses anywhere from thousands to millions of dollars per hour, with 44% of organizations reporting **hourly losses exceeding $1 million**.

WORKFORCE CHALLENGES IN A VOLATILE LANDSCAPE

Workforce instability has become a critical obstacle to growth and efficiency. Businesses are grappling with workforce challenges that disrupt operational flow. High turnover, "quiet quitting," and persistent skill gaps have left IT teams stretched thin, especially as expectations for digital transformation continue to rise. At the same time, many workforce models remain too rigid, preventing organizations from quickly adapting to shifting demands. **This lack of flexibility makes it harder to scale, maintain efficiency, and address emerging risks.**

A report from Korn Ferry estimates that by 2030, the global talent shortage could reach 85 million people, potentially leading to $8.5 trillion in unrealized annual revenues.[4] For IT teams, these shortages aren't just about hiring difficulties—they directly affect service delivery, system security, and the ability to drive innovation.

[3] "What Is the True Cost of Downtime for Businesses?" NinjaOne. (Accessed February 2025).

[4] "The Talent Crunch: Future of Work," Korn Ferry. (Accessed February 2025).

The World Economic Forum has found that two-thirds of organizations face additional risks because of cybersecurity skills shortages, yet only 15% of firms expect cyber skills to significantly ramp up by 2026.[5] As cyber threats grow in complexity, understaffed IT and security teams struggle to keep up, increasing the risk of breaches, downtime, and compliance failures.

To stay ahead, businesses must rethink how they **attract**, **retain**, and **empower** IT talent while also leveraging technology to bridge skill gaps and enhance operational resilience.

The workforce gaps that undermine efficiency

Several key workforce challenges are contributing to these inefficiencies:

- **Talent shortages:** A volatile labor market and increasing demand for specialized IT skills make it harder to retain and recruit talent. According to Gartner®, Many organizations' current workforce models and talent practices are too static, rigid, and slow to effectively keep pace with the needs for digital acceleration."[6]
- **Underutilized automation:** AI and automation have the potential to bridge skill gaps, boost productivity, and reduce manual workloads, yet most organizations lack the systems or strategies to implement these technologies effectively. This leads to missed opportunities to optimize costs and streamline workflows.
- **Siloed teams:** Disconnected workflows and poor communication between IT and business teams create inefficiencies, slow down decision-making, and prevent alignment on critical business goals.

As a result, IT teams are often overburdened, reactive, and unable to collaborate effectively on larger strategic initiatives. Without a modernized workforce strategy that **prioritizes adaptability**, **automation**, and **cross-functional collaboration**, businesses will continue to struggle with inefficiencies, delayed resolutions, and lost revenue opportunities.

OPERATIONAL INEFFICIENCIES AND ESCALATING COMPLEXITY

As IT environments grow more complex, operational inefficiencies are becoming harder to ignore. The shift to cloud-native and hybrid IT architectures has led to sprawling systems that are difficult to monitor and maintain. In fact, 59% of businesses cite application complexity as their greatest challenge.[7]

59% of businesses cite **application complexity** as their greatest challenge.

[5] "Strategic Cybersecurity Talent Framework 2024," World Economic Forum. (Published 2024, Accessed February 2025).

[6] "Reconfigure Your Technology Workforce Model to Be Resilient in Uncertain Times," Shawn Murphy, Lily Mok, et al., Gartner, September 2024 (Accessible to Gartner subscribers only). GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[7] "Driving Outcomes With Observability," SolarWinds. (Accessed February 2025).

At the same time, rising IT workloads are stretching teams thin. According to the SolarWinds State of ITSM Report, organizations managing over 10,000 IT incidents per month face average resolution times exceeding 100 hours if they lack robust tools and processes.[8] Even businesses handling a fraction of that volume struggle to meet SLAs without automation and streamlined workflows.

Key drivers of operational inefficiencies

Several factors contribute to the increasing difficulty of managing IT operations effectively:

- **Reactive problem-solving:** Fragmented systems make it difficult to pinpoint root causes, forcing IT teams to focus on symptom management rather than true problem resolution. Instead of proactively preventing issues, businesses find themselves caught in an endless cycle of firefighting and downtime recovery.
- **Ineffective tools:** Many organizations continue to rely on legacy systems and non-integrated solutions, which require manual coordination across multiple teams and platforms. This not only slows response times but also increases the risk of miscommunication and operational blind spots.

THE TRUE COST OF RESILIENCE GAPS

Resilience has become a strategic imperative for businesses, yet most organizations fall short in their efforts. During the COVID-19 pandemic, many companies scrambled to implement resilience plans that, according to a Gartner research, "By 2026, 80% of the resilience planning introduced under COVID-19 will have failed, been forgotten about or shelved."[9]

By 2026, 80% of the resilience planning introduced under COVID-19 **will have failed**, been forgotten about or shelved.

Why do resilience efforts fail?

- **Lack of strategic alignment:** Many resilience plans are siloed within IT departments, disconnected from broader business objectives like financial stability and customer satisfaction. As per Gartner, "An overwhelming 82% of supply chain leaders indicated that the resources used to improve proactive mitigation, including resilience, were spent on the wrong risks. Worse still, that sense of misaligned use of risk management resources was associated with an 18% decrease in profitability."[10]
- **Inconsistent Investment:** Organizations often overprotect less critical areas while leaving mission-critical functions underfunded and vulnerable to disruption. According to research conducted by Gartner, "While 74% of supply chain leaders felt aligned on how much to spend on proactive mitigation, 45% of supply chain

[8] "State of ITSM Report," SolarWinds. (Accessed February 2025).

[9] "Two Focus Areas to Improve Organizational Resilience," David Gregory, Gartner, April 2024 (Accessible to Gartner subscribers only)

[10] "Executives Align Resilience to the Business to Maximize ROI," Suzie Petrusic, Heather Wheatley, Gartner, September 2024 (Accessible to Gartner subscribers only)

leaders reported faster-than-targeted time to recover after a disruption. Sixty-eight percent reported using less than half of the additional resources they had set aside to respond to disruptions over the past twelve months."[11]

- **Outdated approaches:** Traditional resilience frameworks focus on individual risks rather than preparing for the growing range of global threats, including ransomware, supply chain disruptions, and geopolitical instability.

When businesses fail to build resilience into their entire operational system, they remain vulnerable to disruptions, unable to adapt to changing conditions, and at risk of financial and reputational damage. True resilience requires a **proactive**, **integrated approach** that ensures people, processes, and technology can withstand and respond to ongoing challenges.

THE NEED FOR A UNIFIED SOLUTION

To overcome these challenges, businesses must align their people, processes, and technology. This alignment not only improves day-to-day operations but also ensures the organization can withstand disruptions and adapt to future challenges.

Key strategies for achieving alignment:

- **Break down silos:** Create open communication channels between IT and business units to foster collaboration and align on shared goals.
- **Leverage advanced tools:** AI, automation, and observability platforms can enhance efficiency, reduce downtime, and provide actionable insights, but successful adoption requires more than just implementation—it demands strategy and buy-in. Many organizations struggle not because they lack tools but because they lack a roadmap for adoption or fail to integrate these technologies into existing workflows.
- **Address team adoption challenges:** Without a clear strategy, automation efforts often stall due to resistance to change or uncertainty about how new tools fit into existing workflows. Organizations should focus on educating teams on the benefits of automation, involving them in the adoption process, and ensuring leadership actively champions the transition.
- **Unify systems:** Replace fragmented, legacy tools with a streamlined, end-to-end solution that provides comprehensive visibility into IT operations.

By taking a systematic and people-centric approach, businesses can successfully integrate automation and AI, **ensuring their technology investments drive real impact** rather than becoming underutilized assets.

Without a clear strategy, **automation efforts often stall** due to resistance to change or uncertainty about how new tools fit into existing workflows.

[11] "Executives Align Resilience to the Business to Maximize ROI," Suzie Petrusic, Heather Wheatley, Gartner, September 2024 (Accessible to Gartner subscribers only)