softwareONE

DEFEATING THE BURNOUT EPIDEMIC

How hyper automation and reworked security requirements can help alleviate employee burnout

Employee burnout is at a crisis level, and HR and hiring managers are scrambling to avoid massive turnover. A whopping 95% of workers are thinking about quitting their jobs, primarily because they feel burned out.

What's behind the sharp increase in employee burnout? Last year's rapid shift to remote operations is at least partially to blame. Many companies are still operating on patched together remote networks with disconnected systems and inefficient processes, causing frustration for employees.

These made-fast networks aren't sustainable now that remote and hybrid work environments are becoming the new standard. Additionally, remote work brings inherent security challenges that affect employees' access to their work.

These problems have the potential to grow even more complex as organizations work to harmonize remote and in-office environments. The summer spike in COVID-19 cases from the delta variant pushed many companies to reconsider their return-to-office plans, further cementing the need for continued work-from-home capabilities.

Given the technological pitfalls that still exist in today's work environments, burnout isn't solely on HR to solve — it's also on IT departments and business leaders to streamline business processes that contribute to burnout.

This white paper will explore the process challenges that can cause or accelerate employee burnout. We'll also describe how organizations can **implement hyper automation** and **enhance security requirements** to streamline processes and help reduce burnout.

> **Catastrophic events can put employees in stressful situations that involve lost productivity or lost data, which could contribute to burnout.**

SECTION 1

THE UNSEEN CONNECTIONS BETWEEN BURNOUT, A LACK OF AUTOMATION AND COMPLICATED SECURITY PROTOCOLS

The average workday increased by more than 8% during the pandemic. This additional work time could indicate an increase in the amount of time employees spend on menial tasks, making them feel less valuable as contributors and potentially leading to burnout.

Most companies had to accelerate their digital transformation initiatives to enable remote work. However, many organizations didn't update the time-consuming manual processes and legacy technology systems they relied on to operate. For example, one survey of treasurers found that manual processes, including the outdated use of faxes, created unnecessary complexities during the pandemic, with 93% of respondents citing a lack of automation as the culprit.

In a separate survey of supply chain executives, 43% said their operational systems lacked automation planning and optimization, hindering their ability to make informed and coordinated decisions in response to COVID-19 disruptions. Additionally, 28% of respondents said their system is completely manual with no system support. Most respondents also indicated their organizations use spreadsheets to manage complex workflows.

Security issues also contributed to burnout for employees in remote and hybrid environments. Before the pandemic, organizations typically protected data within the four walls of their office, but remote work broke those barriers down. Now, data is much more fluid, moving between different locations as employees shuttle between work and home or take their laptops even further afield, across state and national boundaries.

Some companies have been reluctant to move processes from physical servers into the cloud, creating backlogs and delays that many organizations are still dealing with. Even when companies were willing to shift processes off-premise, complex security requirements hindered employee access to data and information. For example, many companies enable employees to access certain information on company-owned devices, but restrict that same access on personal mobile devices. This inability to access work materials can lead to employee frustration when forced to work in an inflexible environment.

Another security issue that possibly contributed to employee burnout is weak data backup protocols from organizations. Although 90% of companies back up data, only 41% back it up daily, indicating that many organizations only rely on their cloud provider's weekly required backup that's built into the provider's service-oriented architecture (SOA). However, remote and hybrid work environments increase the risk of cyberattacks. Instead of employees using company-owned devices on a secure single company network, they're now logging in from personal devices on multiple networks — including the insecure WiFi of a local coffee shop.

This lack of data backup combined with the security implications of remote and hybrid environments leaves organizations at greater risk for highly damaging cyberattacks. Catastrophic events can put employees in stressful situations that involve lost productivity or lost data, which could contribute to burnout.

Some companies have been reluctant to move processes from physical servers into the cloud, creating backlogs and delays that many organizations are still dealing with.

AUTOMATION VS HYPER AUTOMATION

Automation

Technology that enables processes to be completed more efficiently

Hyper Automation

A framework of multiple technologies unique to a company's needs that help automate organizational processes

SECTION 2

COMBATING EMPLOYEE BURNOUT WITH STREAMLINED HYPER AUTOMATION AND SECURITY

Organizations can't ignore the effects a lack of automation and challenging security requirements can have on employee burnout. As you determine how to optimize your remote or hybrid work environment for long-term success, consider how you can adopt hyper automation and revamp your security to stop employee burnout before it begins.

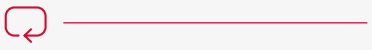
Keys to hyper automation

Consider the following when implementing hyper automation within your organization's processes to achieve greater operational efficiency and free up time for employees to focus on more engaging, high-value tasks:

1. Use process nomination

Most automation is rules-based — the technology executes a task in response to a certain action. So, a process must be well-defined for a bot to execute it in place of a human worker.

We recommend asking three questions to determine if a process is suitable for automation:



Is it repetitive?
A bot should be able to execute the process repeatedly without diversion or complex steps.

Is the process high-resource and mundane?
Identify tasks that take a long time and require effort from multiple employees. For example, invoice processing can require the time and effort of many workers, so determine where time can be given back to these groups of employees.

Is it 24/7?
Typically, processes that require 24/7 support require too much time from employee resources, so determine which portions of these constant actions can be covered with automation.

2. Walk before you run

Accelerate your use of automation over time. Many organizations want to leverage complex solutions like artificial intelligence (AI) and machine learning (ML) at the beginning of their foray into automation. However, you should consider how base-level uses of automation such as low-code, business process automation and trigger flows can shore up certain processes first — especially ones that affect employees' time the most.

SoftwareONE's Hyper Automation Services can help you automate processes by building the right hyper automation framework for your organization. This specialized offering can help your employees save time so they can focus on high-value tasks, reducing burnout.

SoftwareONE can work with your team, including IT and department leaders, to help identify which processes are ripe for automation within your organization through our User Productivity Solutions.

Factors for enhanced security

Security requirements have evolved for remote and hybrid environments — but they can't hinder employees' ability to work.

Consider the following principles to level up your security strategy:

Consider a bring-your-own-device (BYOD) solution

Expand your security requirements to enable access from employees' personal devices for remote work with a BYOD security solution. For example, you could implement a technology that containerizes company data within an employee's personal device to keep it separate from their personal data. And if the device is compromised or the employee leaves the company, the containerized environment enables you to securely wipe your company's data from the device without impacting the employee's personal information. This security technology can offer a necessary level of protection while creating minimal impact on employee access when employees use their own devices.

SoftwareONE's Workplace Security Professional Services can build a strategy roadmap to secure your remote workforce and simplify end-user access while ensuring business continuity in a fully remote or hybrid work environment. A key component of our BYOD approach is Microsoft Intune delivery. This solution leverages top-level privacy and security methodologies to control how network users access and share information, helping keep data backed up and protected no matter what device is used in your network.

Prepare for the worst in data breaches

Data backup needs to be a priority in remote and hybrid work environments with ransomware attacks on the rise and the ongoing risks posed by other cybersecurity threats. Too often, companies assume any data they store in the cloud with a reputable provider is backed up "enough." But relying on your cloud provider's weekly backups alone only increases your risk of a catastrophic data loss that can negatively impact employees' work lives.

Take control of your data by making it your responsibility. Double down by enacting your own backup protocols outside of the required procedures of your cloud provider's SOA. Should you experience a catastrophic event, more frequent and strategic data backups can help your employees restore their work with minimized friction.

With SoftwareONE's BackupSimple powered by Metallic solution, you can ensure data is recoverable in the event of ransomware attacks and other data loss events. This offering protects multiple data types no matter where it's stored — including hybrid cloud datacenter workloads, SaaS apps and endpoints — with a single tool.

SET UP EMPLOYEES TO THRIVE WITH A MODERNIZED DIGITAL WORKPLACE

Are you ready to transform your business processes for more secure and efficient operations that positively impact your employees and company? Don't let broken processes and complicated security requirements accelerate a burned-out workforce.

Book a digital workplace advisory meeting today to see how we can empower your hybrid workforce.

softwareONE

20875 Crossroads Circle,
Suite 1, Waukesha, WI 53186
sales@softwareone.com
+1 800 444 9890

SoftwareONE

SoftwareONE is a leading global provider of end-to-end software and cloud technology solutions. It enables commercial, technology and digital transformations using IP and technology-driven services. Clients can modernize applications and migrate critical workloads on public clouds while optimizing their related software and cloud assets and licensing in parallel.