

# The impact of IT operations automation on the morale, productivity, and security posture of IT teams



## CONTENTS

Introductory remarks .....	2
Methodology.....	2
Knowledge of automation tools and strategy.....	4
Reducing human error and increasing productivity .....	5
Boosting IT team morale .....	6
Automation's impact on security and risk.....	7
Preparing for an automated future.....	9
Tanium Autonomous Endpoint Management.....	10

## Introductory remarks

**Automation has the capacity to transform the way IT teams operate, from automated threat hunting to automated patching. However, not all organisations are making the most of its capabilities. In fact, many IT professionals are suffering from ineffective efforts to incorporate automation into their processes.**

The following report analyses research conducted by PureProfile on behalf of **Tanium** and aims to unveil the real-world and business impacts of IT operations automation on the morale, productivity, and security posture of IT teams.

The survey results reveal a pressing need to address knowledge gaps, communications gaps, and operational inefficiencies within organisations, particularly regarding automation and workload management. For example, the data suggests a strong foundation of automation awareness among C-suite respondents, with 100% rating their knowledge of automation tools as good or very good, compared to only 44% of non-managerial staff. There are also clear disparities between the C-Suite and IT teams' views on budget, culture, and tool adequacy.

The findings emphasise that automation can lead to better productivity, and security while also reducing employee burnout. To achieve these outcomes, there is an urgent need for a cohesive automation strategy that is inclusive of the workforce's operational needs and aspirations.

## Methodology

The research was commissioned by Tanium and conducted by PureProfile between the 8th of October and the 15th of October 2024, surveying 110 Australian-based professionals working at companies employing over 1,000 people. All respondents have influence or decision-making authority over IT hardware and/or IT solutions and have visibility into or involvement with the delivery of their organisation's endpoint management and security program.

# Key findings

 **75%**

Over three-quarters of IT workers say automation tools could improve overall security by shortening patch cycles, reducing vulnerability exposure timeframes, and lessening time spent on incident response.



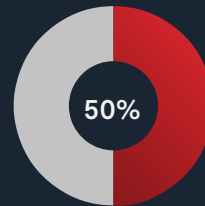
Human error causes almost half of IT teams to spend between 1.6 and 2.9 days per month fixing mistakes.

 **3 Days**

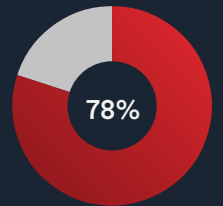
17% of IT workers spend a minimum of three days fixing mistakes, which has a major impact on productivity and security.

The C-suite underestimates how long IT teams are spending fixing human errors:

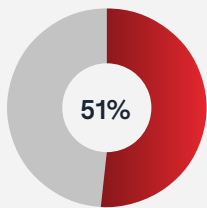
- 50% of C-suite estimated organisations spend 0-10 hours
- While 78% of those at a general manager (GM) level estimated 11-20 hours
- With only 11% of GMs estimating 0-10 hours spent



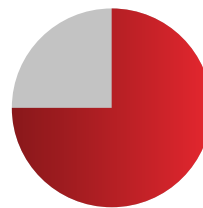
0-10 hours for CIOs



11-20 hours for GMs



Around half of IT workers would support automation if it meant they could work less time out of normal hours.



Almost three-quarters of IT workers want to adopt automation tools so they can work on more meaningful projects.

IT professionals believe budget is the biggest inhibitor of automation adoption, followed by company culture

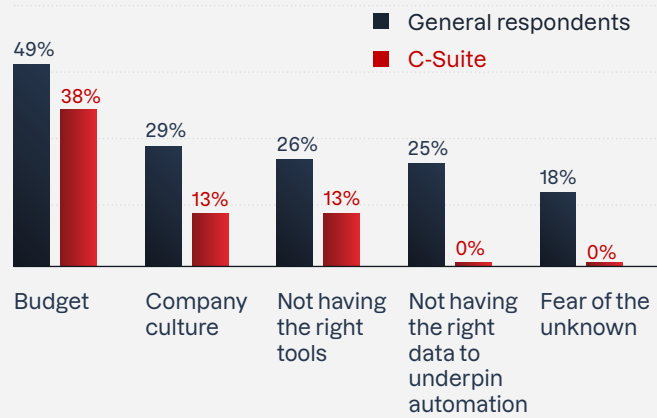


**69%**

experienced burnout

Three-quarters of IT workers say automation could help reduce burnout, which is experienced by 69% of IT teams.

## Whats holding businesses back?



## Knowledge of automation tools and strategy

At first glance, it may seem like the C-Suite and IT teams within businesses are on the same page regarding automation tools and strategies. However, taking a closer look reveals a significant disconnect.

While 100% of C-Suite executives rated their familiarity with tools as 'good' or 'very good', only 44% of those in non-managerial roles felt the same. Furthermore, a mere 18% of respondents said they were going ahead with implementing automation to a greater extent, in comparison to a whopping 63% of C-Suite respondents.

These major gaps highlight a range of challenges businesses cannot afford to overlook. The C-Suite is expected to build and communicate operational automation strategies while also adequately equipping teams to bring those strategies to life. However, the data demonstrates this is rarely the case, with many IT teams out of the loop. Furthermore, a quarter of teams feel they do not have the right tools (26%) or the right data to underpin automation (25%) to be able to bring automation strategies to life.

The research also points to significant differences between what the C-Suite and IT teams see as the biggest barriers to implementing automation to a greater extent.

There is a clear opportunity for business leaders and executives to improve the way they communicate their operations' automation strategies while also empowering teams to make the most of the automation tools available. This could include:

- More regular online or in-person updates from the C-Suite
- Incorporating updates into 1-1 managerial catch-ups and team meetings within IT departments
- Bespoke training for IT teams to understand the over-arching strategies and how to approach their role within relevant action plans
- Company-wide announcements specifically about automation from the C-Suite that highlight any changes or updates in the business strategy
- Open Q&A sessions between the C-Suite and IT teams directly impacted by automation strategies
- Team-wide feedback sessions for IT professionals to share what is going well and what could be improved
- HR-led discussions to better understand the potential and limitations of the current company culture and the impact on automation strategies
- Cross-collaborative efforts between departments to equip IT teams with the right data needed to implement automation strategies effectively



Almost half of IT teams are spending between 1.6 and 2.9 days per month fixing human errors

### Key benefits of effective operational automation

- Increased operational efficiency through automation of routine tasks
- Enabling teams to do more with less, redirecting day-to-day time spent on manual tasks to focus on growth initiatives without compromising security performance or availability
- Improved security posture with accelerated risk mitigation by proactively managing vulnerabilities and incidents
- Improved team morale while reducing burnout, which can increase employee engagement and reduce staff turnover

## Reducing human error and increasing productivity

Recent major data breaches and outages around the world have highlighted the potential for a single human error to bring hundreds of businesses to a standstill. Human errors within an IT environment can have significant ramifications on network performance, digital experience, security integrity, and more. This is why correcting human errors as quickly and efficiently as possible is integral to forming a high-performing company.

However, too much time spent fixing human errors can take critical resources away from completing strategic work and impact an organisation's overall productivity. Unfortunately, this is what's happening in IT teams across Australia, with many spending the equivalent of an entire month fixing human errors.

The research uncovered that almost half of IT teams are spending between 1.6 and 2.9 days per month fixing human errors, which is the equivalent of between 19.2 and 34.8 days every year. For 17% of IT teams, human errors take up at least 10% of their time, spending a minimum of three days on this every month.

To make matters worse, this significant drain on time and resources is often being drastically underestimated by the C-Suite. Half of executives estimate organisations spend only 0-10 hours on human errors, while 78% of those at the general manager level estimated 11-20 hours are spent on human errors each month.

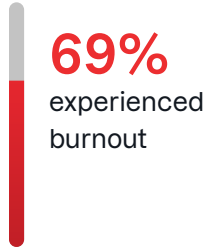
The issue is more severe in larger organisations. In organisations with 1,000-4,999 employees, only 2% of respondents claimed they spent more than 10 days per month fixing human errors, whereas this was the case for 16% of organisations with 10,000 or more employees.

Automation tools hold many solutions to the hundreds of hours IT teams spend on fixing human errors. With businesses under constant pressure to "do more with less," automation can ensure skilled resources are appropriately delegated to skilled jobs, while automation takes over correcting human errors and completing administrative tasks that require minimal skills.



## Boosting IT team morale

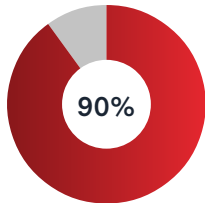
IT teams are hard workers. The research highlights that their dedication at work is not only costing them significantly in terms of time away from loved ones and their personal lives but also impacting their overall morale and motivation in the workplace.



One-third of IT teams spend 5-15 hours every week on scheduled activities outside of regular hours, and 15% of IT teams spend over 16 hours per week. More than two-thirds (69%) of survey respondents said they or someone in their team has experienced burnout in the last six months due to workload and/or working out of normal hours. Of those, 75% said they believe this burnout could have been avoided if manual and repetitive tasks could be automated.

### Burnout by industry:

Respondents reporting they or someone in their team has experienced burnout within the last six months due to workload or working out of normal hours



**Overall, 90% of respondents noted that manual, repetitive tasks impact workforce morale**

Again, there is a clear discrepancy between how IT teams and the C-Suite view the role of automation on this issue. More than half (51%) of respondents said they would support automation if it meant they or their team could work less time out of normal hours, though this was the same for only 13% of C-Suite respondents. Meanwhile, only 2% of overall respondents said no to supporting automation because they are happy with their current projects, tasks and the hours they work, while 13% of the C-Suite felt the same.

Low morale and employee satisfaction can quickly lead to poor company culture, high staff turnover, and significant impacts on the business's bottom line. Furthermore, time spent working out-of-hours typically involves time off work during hours, pulling skilled employees away from value-adding tasks, and further impacting business productivity and profitability.

Importantly, for IT teams, the cost of burnout is not just an HR issue. It's a security issue, too. Teams that have a full mental load or are feeling emotionally or physically tired are more likely to make mistakes, overlook minor errors by peers, or raise important concerns internally that could lead to further work. Each of these outcomes creates more risk for the business, opening the security gates to even more human errors, breaches, or attacks.

In many scenarios, automation could replace work that specifically needs to be done outside of standard office hours. This includes patching done with legacy tools. Modern patching tools do not impact performance and, therefore, do not need to be used out of hours, freeing IT teams up to patch faster, more effectively, and in ways that enable stronger work-life balance and overall well-being.


## Automation's impact on security and risk

As businesses and IT professionals continue to explore and invest in AI and automation tools, the research highlights clear gaps in how these journeys are taking place, as well as the financial, HR, cultural, and productivity impacts of not getting it right.

One of the biggest business challenges is overcoming the security risks of delaying or ineffectively implementing automation strategies. As security threats continue to rise from external bad actors, the ongoing increase in the volume of devices and endpoints connected to every business means the risks from internal staff or third parties connected to the business are also exponentially growing day by day.

As the data demonstrates, the mountain of human error that IT teams are continuously managing is unsustainable. As threats continue to rise, there will be less and less time to fix errors and an insurmountable security debt, exposing organisations to significant risk with the threat of both financial and reputational damage.

Automation tools are proven to free up significant time and resources for IT teams, which in turn alleviates the pressure and stress associated with their jobs. This can lead to stronger employee engagement and more time available for innovative or proactive tasks that can help grow the business.



Over  
**3/4**  
say automation  
tools could  
improve  
overall security

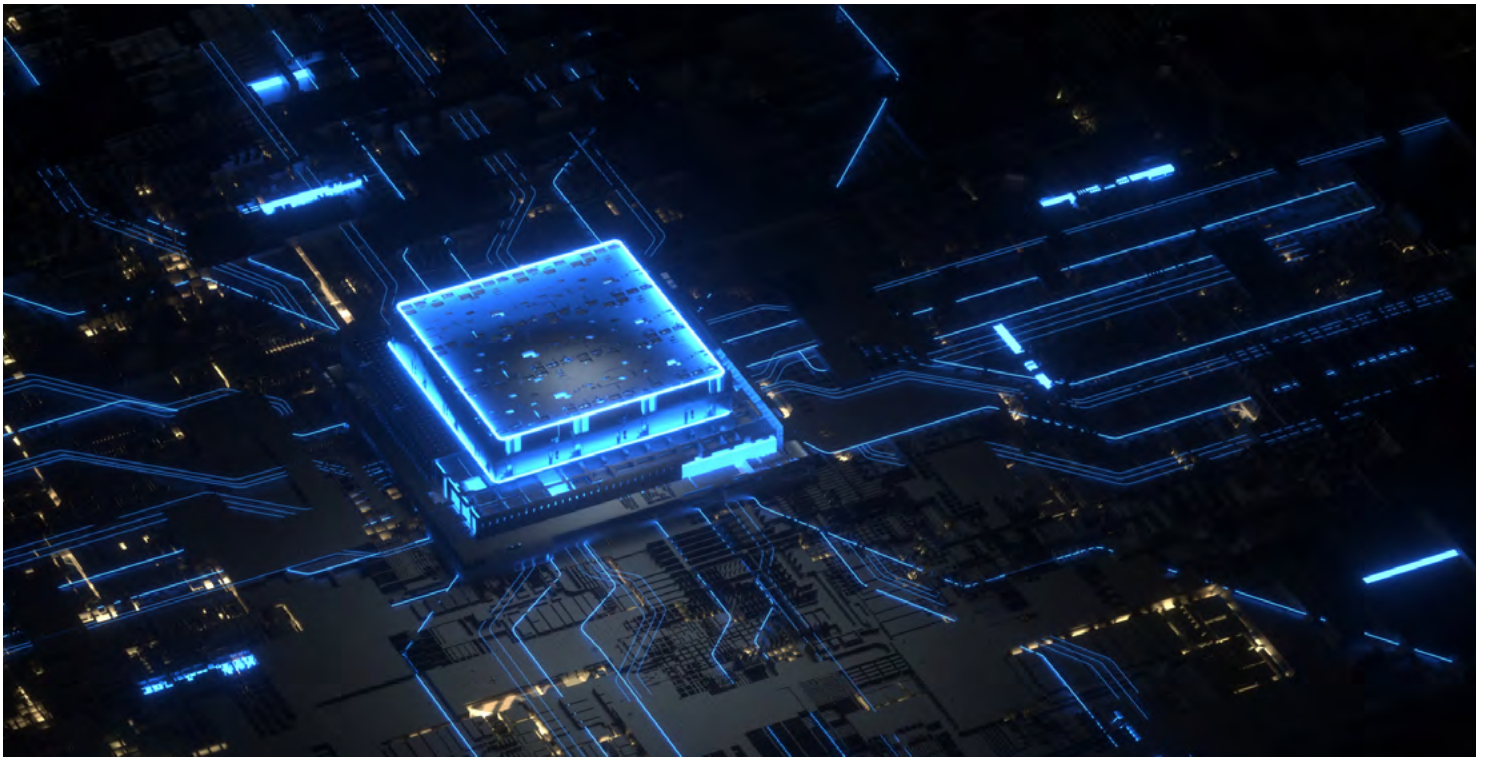
According to the research, over three-quarters of IT workers say automation tools could improve overall security by shortening patch cycles, reducing vulnerability exposure timeframes, and lessening the amount of time spent on incident response.

For C-Suite executives, this should be a wake-up call. While there are clear challenges that all businesses face with AI and automation, no business can afford to overlook the real daily pressures and risks that IT teams are facing as they call out for stronger communications, investments, and commitments to automation strategies that work.

## How businesses can turn challenges into opportunities:

Challenge	Opportunity
<p>IT teams are overwhelmed by the amount of manual work required to keep endpoints, operating systems, and applications up to date.</p>	<p>Leverage automation to lower the volume of manual work, enabling teams to achieve previously unattainable outcomes.</p>
<p>The growing volume and complexity of cyberattacks means IT teams need to patch faster, have better device configurations, and address vulnerabilities faster.</p>	<p>Use automation to reduce mean time to remediate metrics to combat growing risks.</p>
<p>AI and automation are complex and time-consuming to implement.</p>	<p>Look for tools that use low code/no code options to enable simpler implementations. Following the one-time setup, there will be long-term benefits, including minimal monitoring required in comparison to previous, ongoing manual efforts.</p>
<p>Businesses lack real-time data for reliable outcomes.</p>	<p>Implement tools and processes that utilise real-time data, which is significantly more reliable than point-in-time data and can be used to drive decision-making without the doubt often associated with historical data.</p>
<p>Significant developer resources and time are needed to integrate multiple tools.</p>	<p>Leverage platforms with a low code/no code automation layer that performs multiple tasks to greatly reduce this overhead.</p>
<p>Businesses could potentially introduce more risk without tight controls and data reliability.</p>	<p>Using tools that provide inbuilt confidence scoring based on historical data at scale can help to futureproof a business and mitigate risk.</p>
<p>Highly skilled experts are needed to build out automation libraries.</p>	<p>Automation can provide career advancement and training opportunities for skilled staff who, once proficient, can pass these tasks on to more junior staff to operate.</p>





## Preparing for an automated future

Most Australian businesses recognise that an automated future is worth working towards, though the race to automation will inevitably have a range of 'winners' and 'losers'.

Those that lag behind will be dealing with mounting human errors and the excessive resources required to address them, as well as the significant security risks that come with manual processes and a burnt-out workforce. Organisations leading the race, however, will take proactive measures to use automation strategically, with a focus on enabling IT teams to work on the highest value work possible while contributing to the growth, future-proofing, and innovation of the organisation.

As businesses continue to invest in AI and automation tools, it will be critical to regularly take stock. While automated processes can encourage a 'set and forget' mindset, automation strategies themselves should be periodically assessed for their effectiveness. This includes analysing how the automation tools are being used, the efficiency of those tools in freeing up resources and adding value to the business, and whether the tools effectively contribute to the organisation's overall automation strategy. It is then in the hands of executives and leadership teams to continuously improve their automation strategies and communicate these improvements company-wide on a regular basis.

# Tanium Autonomous Endpoint Management

Tanium Autonomous Endpoint Management (AEM) delivers autonomous management of endpoints across the industry's most comprehensive platform, providing solutions for asset discovery and inventory, vulnerability management, endpoint management, incident response, risk and compliance, and digital employee experience.

Tanium AEM leverages real-time insights from Tanium cloud-managed endpoints to recommend and automate changes on endpoints within a customer's environment, giving IT and security teams a safe, scalable, and automated platform to deliver increasingly efficient operations and an improved security posture at scale, with confidence, and in real time.

## **Tanium Automate - Orchestrate and automate mission-critical tasks with confidence**

With Tanium Automate, a key component of Tanium AEM, your IT and security team can easily create custom playbooks – with little to no code – to automate any IT challenge. Automate's orchestration capabilities keep your team informed and in control, so that changes can be rolled out into your environment with confidence and certainty.

- Automate time-consuming manual tasks
- Accurate, high-confidence execution
- Complete control and confidence

**Learn more here →**



**→ [www.tanium.com/products/tanium-automate/](https://www.tanium.com/products/tanium-automate/)**

**Get in touch with our team today to learn more about how Tanium AEM can help you improve morale, productivity, and security across your IT team.**

**Contact us here →**



**→ [www.tanium.com/contact-us](https://www.tanium.com/contact-us)**