CAE
TECHNOLOGY ON POINT

The enjoyment index for IT leaders and professionals
CAE 2022 Research Findings

What's holding back **more good days in IT security?**

> thisiscae.com

Contents

Executive summary

This is not a story that shines a light on unsung heroes. Most businesses today are more than aware of IT's role for keeping them safe, productive, and able to confidently engage with the outside world. But it is a story that explores the satisfaction levels of IT security professionals, and those factors that can make for a bad day at work.

These are points that need highlighting. **Particularly when 21% of those surveyed for this report suggest that experiencing a stressful day in the office has become routine** – a number that grows to 27% for IT leaders. What's more, this is a day that for 65% of respondents typically grows into a work week of 40 hours or more – despite only 38% being contracted to work that amount of time. Being overworked therefore remains an issue, and is undoubtedly tied to **the opinion voiced by three in five respondents that their employer's demands have gone up over the last 5 years.**

At the same time, **53% of IT leaders report feeling more stressed about security concerns at work.** Which is unsurprising given the fact that 92% consider the threat level to have increased in recent times, driven by factors ranging from the surge in remote working and global political tensions, to more cloud usage and smarter hackers.

Added to this is the growing view that companies are not providing sufficient training or resources to cope with the introduction of new technologies. An opinion now shared by one in three respondents, though here a marked discrepancy exists between the view of IT leaders (where 75% believe the right level of resources/training is in place) and IT professionals (where only 57% agree). Therefore, it seems inevitable that our research finds **the number of IT leaders who consider themselves 'appreciated' hovering at the 72% mark**, and dropping to 69% for IT professionals.

Not that it's all doom and gloom, as the report also offers pointers for how to dial up more good days. Good examples here being the fact that **24% of all respondents complain of too many boring/repetitive tasks, their roles being too stressful (23%)**, and limits on career progression (20%). Plus, there are those elements already inspiring a more positive outlook, including pay (44%), job security (38%), and interesting work (34%).

All told, the survey's findings point to a time of transition in IT circles, as workers seek smarter, more automated security tools to relieve them of more monotonous tasks – and to open up the more proactive and strategic aspects of their roles. **The challenge is being set, and at CAE we're blazing a trail from the mundane to the marvellous with smarter, intelligent technology that transforms user experiences – and helps deliver more good days at work.**

Introduction:

A growing number of technology brains are being numbed by the daily grind

Few IT and security professionals will mourn the passing of the 2022 work year.

A similar sense of "good riddance" will accompany the end of the year as it did in 2021. Hope springs eternal that next year will be better, yet in reality IT workers continue to show a low intent to stay in their current roles – when compared that is to workers in other sectors. The result being a 'brain drain' that's helping remove one of the most potent barriers to any potential security threat: experienced heads who know your systems inside and out.

People whose loyalty has been eroded by one simple fact: the bad days they have at work can too often outweigh the good ones.

That means less smiles and more frowns. Where one quarter of those involved regularly have a day to forget. Driven by too many boring or repetitive tasks, stressful situations, and a distinct lack of unified, joined-up team work. All this at a time when security threats continue to adapt and mutate. Demanding a response in terms of new tools, new skills, and new thinking that is best delivered by a fully motivated and positively-minded workforce.

This of course has always been the case. And as we know there is a direct correlation between IT security capabilities, and the level of skill and experience pulsing through the team responsible for maintaining them. That's why uncovering the factors that lead to bad days as well as the wider factors impacting morale, is a mission that now carries with it a greater sense of urgency.

This report was commissioned with that goal in mind. To discover what's really going on in the day-to-day to cause frustration, irritation, and annoyance.

CAE does this with a clear purpose in mind. Happier, more empowered people are better for your business and ours. We imagine a world that reduces the mundane and boring tasks to an absolute minimum. Freeing up IT teams to focus on the tasks that get them buzzing and working at their very best. Likewise, our clients have an ambition to unleash their talent on activities that deliver long-term business value. It's a shared endeavour that acts as a central idea running through this report.

By reading on you'll find the problem brought to life and areas highlighted where even small improvements can make a big difference.

So let's get started...

But what's contributing to **bad days in IT?**

Is security a source of satisfaction or discontent?

7.83

The average score for each organisation's overall approach to IT security

The headline here is that two out of three respondents **(66%)** rate their organisation's security approach as positive. A good vibe for sure, and particularly so when supported by other key findings:

> 98% believe their organisation is protected (versus unprotected) against a potential security threat

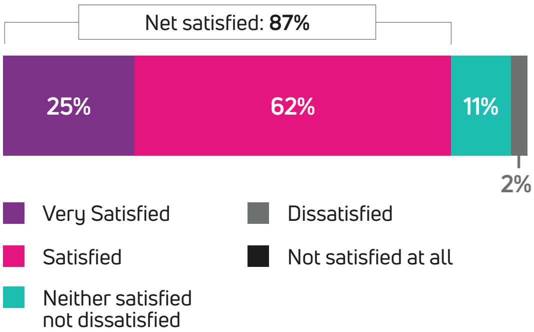
> 94% have confidence in their organisation's ability to recover from a ransomware attack

That said, we need to find an explanation for why a third rated their organisation's response as either neutral **(31%)** or negative **(2%)**.

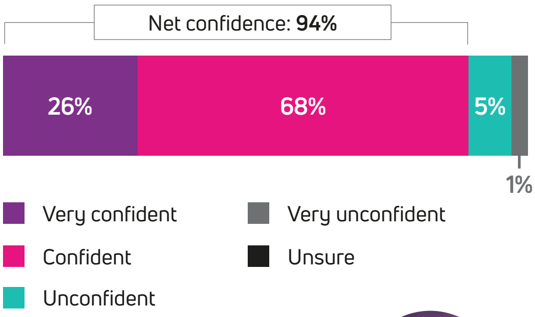
Dissatisfaction with the existing security stack could be one area to explore, though in reality 87% of respondents rated their current set-up as 'satisfactory'.

Arguably, a more direct contributor to a bad day is the level of mundane, repetitive tasks involved (impacting **27%** of IT professionals), that bring with them a heavy element of boredom. Worse, by taking up so much time, expert IT resource is denied the thinking space it needs to consider and/or maintain a more proactive defensive stance.

Levels of satisfaction with existing security arrangements



The confidence of being able to resist a ransomware attack



A frustrating skills gap has appeared (and it's not going away any time soon)

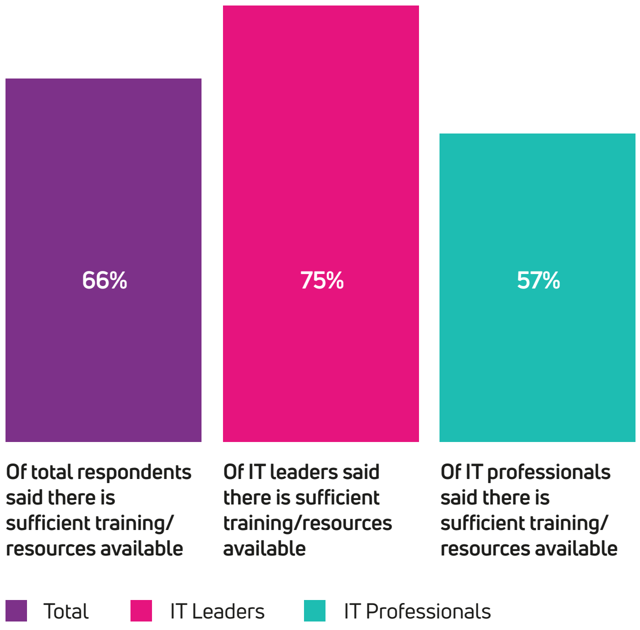
There are two sides to this gap. On one side is the resourcing issue, while the other relates to training levels and certification. The absence of either can directly cause people to become swamped or left performing more junior roles that fail to generate any sense of long-term excitement.

When it comes to resourcing, there is a growing skills deficit in cybersecurity across the globe. This in turn can lead to problems such as unconfigured systems, tardy patching, lack of oversight, insufficient risk assessment, and rushed deployments. It's no wonder then that the World Economic Forum has stated that 60% of organisations would find it "challenging to respond to a cyber threat". A skills gap quantified in part by the Department of Culture, Media and Sport (DCMS) which is predicting an annual shortfall of 14,000 for entrants into the cybersecurity market.

Our findings show that only 57% of IT professionals believe there is sufficient training and resources available to support them on a daily basis.

As for training, the immediate concern is likely centred on organisations not offering or supporting access to courses that help teams expand their CISSP certification (or equivalent). Yet in reality, the source of a bad day is in how a lack of training and certification dictates the tasks each team member is asked to complete. This can quickly lead to people having either an under or overabundance of work to complete, with specific jobs being consistently passed to the same individuals – thus further contributing to a sense of repetition and the lack of motivation that slowly comes with a 'Groundhog Day' experience.

Do you believe there is sufficient training and resources available to cope with new technology?



No one wants to feel like an afterthought

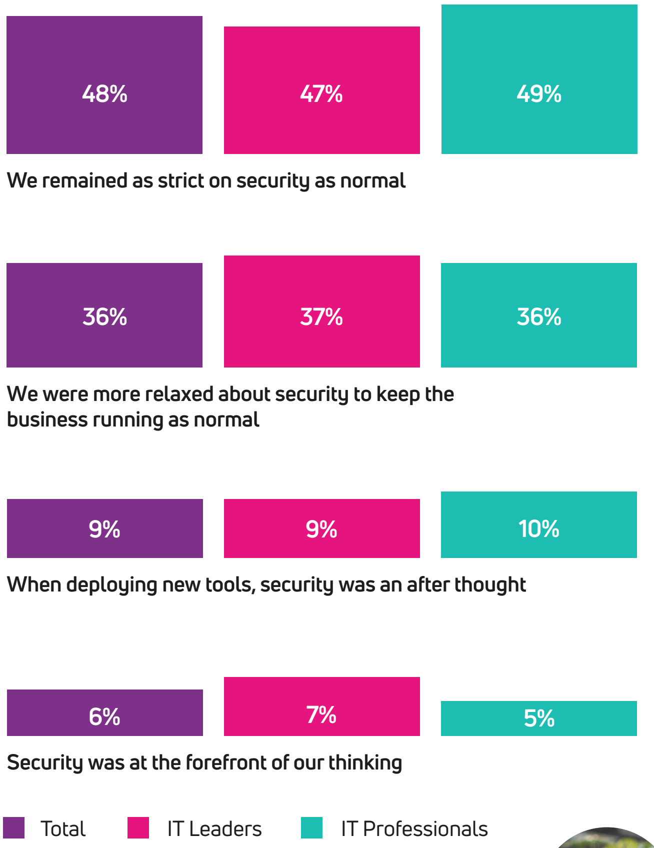
Another key cause of bad days at work is that sense of being isolated from strategic priorities, and being brought in only after the big decisions have already been made. For example, in recent times the need to enable remote working in a bid to maintain employee productivity has been hurriedly placed at the feet of many an IT function. Keeping people working, creating, and collaborating is the urgent outcome required – with security often relegated to a secondary consideration.

Indeed, our findings suggest that 45% of organisations are now more relaxed – or that security was an afterthought – when deploying new tools. Possibly an even bigger headline to note is that **only 7% of respondents believe security is at the forefront of their organisation's thinking.**

This is of course a source of deep-rooted frustration in IT circles. Tasked with securing the organisation from multiple, highly sophisticated attack vectors (and being among the first to receive blame for any successful penetration), IT has long recognised that for effective protection the topic must remain a front of mind concern. Holistic and fully integrated being the buzzwords at play here. Yet the evidence points to a situation where the delivery of new tools and technologies is signed off as a fait accompli, before any thought is given to the associated security implications.

The survey supports this view, with 27% of IT leaders claiming a lack of cohesion with the rest of the business. Meaning that efforts to educate and enforce a 'security-first' mindset still has a long way to go, which in turn points to familiar problems ahead – as well as the same maddening conversations.

Do you believe security is at the forefront of your organisation's thinking?



Curb your enthusiasm

Weight of expectation is another burden drooping the shoulders of IT teams. **In fact, three in five claim that these expectations have risen over the last five years.**

Partly, this increase is put down to the ever-growing security threat – and the need to enable the 'new normal' world of remote working. But side-by-side with this demand comes the assumption that IT retains expertise in any subject relating to technology.

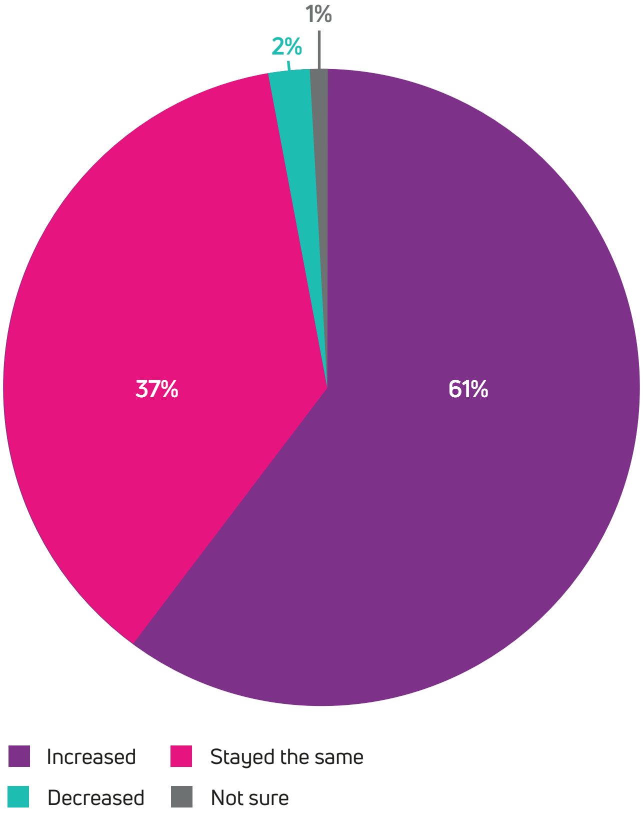
> **"The expectations are that we instantly know and understand all new products and services available",** noted one respondent. While another commented that her organisation is **"much more demanding of better and more sophisticated equipment, faster responses, and better technology".**

IT should of course be a repository of technical know-how. But what comes across strongly in the survey findings is the limited understanding that exists higher up the organisational chart. A reality exposed in the data, which shows that the tasks being set for IT often cause a conflict with their core priorities. This situation in turn requires IT leaders to constantly struggle in the effort of educating their executives on the real-world impact a security breach can have on customers, operations, and reputation.

In addition, the mission set IT has expanded from a core of three to five keys tasks to now incorporating aspects such as GDPR and empowering the workforce. As a result, the function of security is frequently broken down into a series of isolated business problems, rather than being addressed via a top-down strategic approach.

Where a more holistic view is adopted, IT leaders are applying the concept of zero trust to securing data and client devices. A position that for a growing number means embracing the protection offered by an end-to-end security foundation that incorporates the network, identity, endpoints, data & applications, analytics, and response.

Have your employer's expectations changed over the last five years?



What's the source of plain and mundane?

IT professionals and leaders are clearly a passionate crowd. They love the fundamentals of what they do. A remit that is truly end-to-end given the demands of enforcing a zero-trust architecture approach.

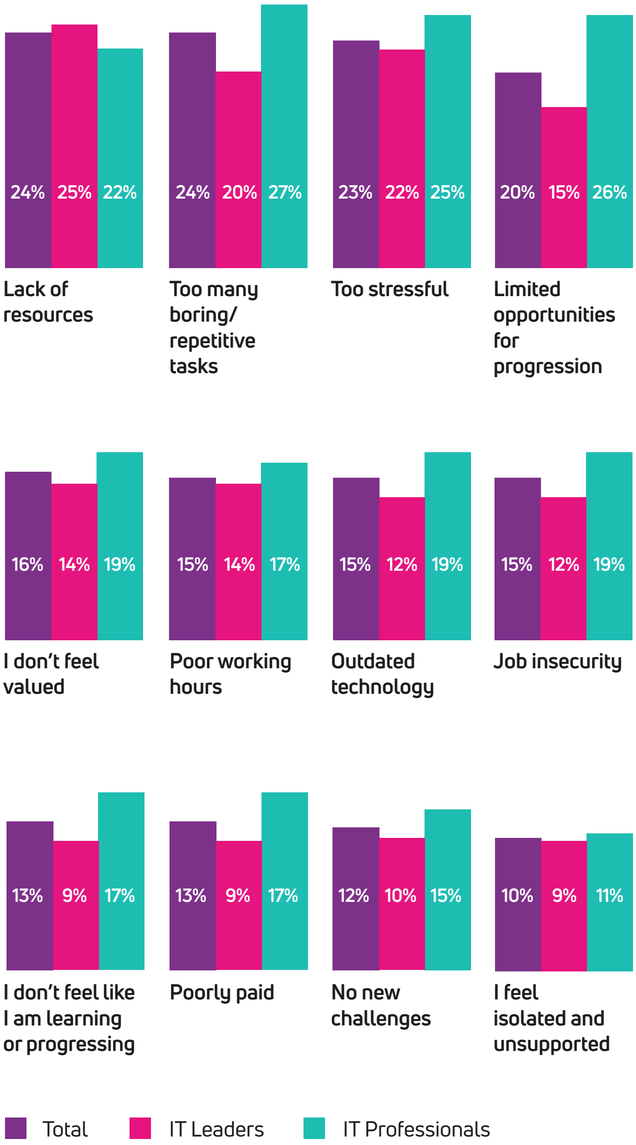
Maintaining this desire is obviously important, and this survey helps shed light on those issues that can turn a good day into an instantly forgettable one. **To start with, there is the lack of resource issue, which was emphasised by 25% of IT leaders.**

For IT professionals though, t**he biggest gripe was the need to complete too many boring and/or repetitive tasks (27%).** A result that narrowly beat the apparent lack of opportunities for progression (26%), and the workplace proving excessively stressful (25%).

Two other results worthy of mention is that **nearly one on five (19%) IT professionals don't feel valued,** with the same amount also grumbling about the limitations of outdated technology.

Overall, there's a detectable sense that skilled resources are not able to fulfil their potential due to a lack of training and certification as well as the time spent on routine tasks. Combined, this situation is having a significant impact on morale. Bringing back the happy, therefore, calls for a transformation is SecOps, aimed at unleashing employee productivity and giving them the control needed to utilise their talent, learn, and grow. The goal being to free up IT resource to focus on more rewarding challenges and activities, which in turn leads to a more secure operation – and more good days for both staff and the company.

What are the most negative aspects of the IT security role?



It’s time to find the good

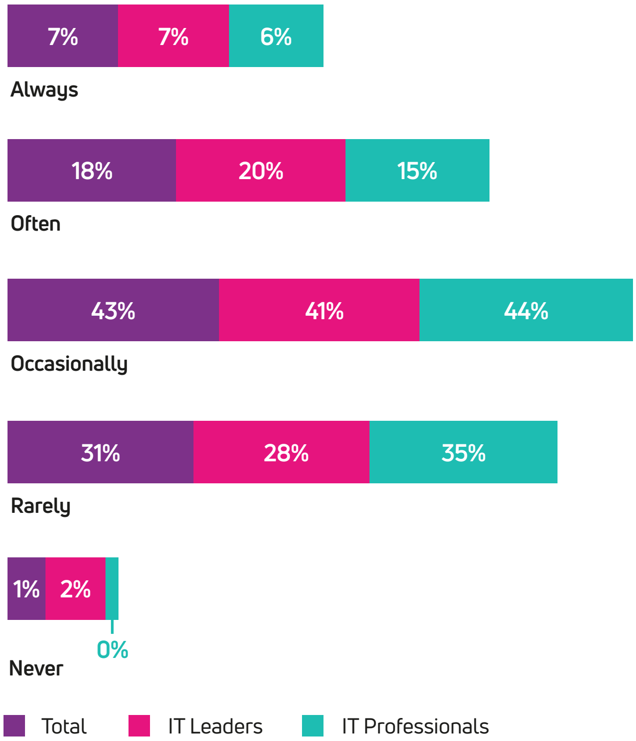
Bad days for IT security professionals occur a lot more often than you probably think. The good news though is that overall, 28% of those surveyed suggest a bad 24 hours happens “rarely” – with 2% answering “never”.

But not everybody is experiencing good days as standard. **In fact, 27% of IT leaders say they “always” or “often” have a bad day at work,** with 21% of IT professionals having the same opinion.

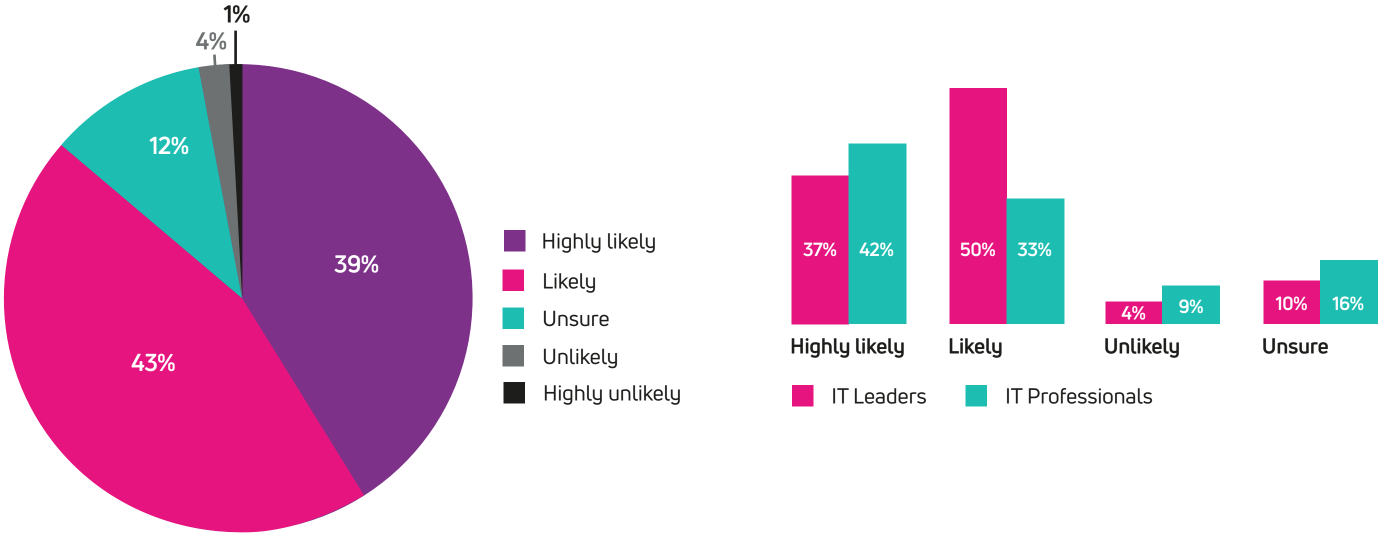
The key factors contributing to this situation have, at least from a high-level perspective, been touched on in previous pages. From low resource availability and limited training opportunities, to mundane tasks and the speed of digital transformation, much exists to counter even the most positive of outlooks.

The net result of such frustration is an anticipated desire for change. However, our results show that a healthy majority of IT talent is determined to ‘stick it out’ in the short term. **This is evident from the finding that 82% of respondents said they were likely to remain in their job over the next six months.** Such a statistic points to an end of the ‘great resignation’ seen in recent years, and provides further encouragement for companies to increase investment in the people they have to ensure they feel valued and content.

How often, if at all, do you have a bad day at work?



How likely are you to stay in your job over the next six months?



Summing it all up

Making more good days a reality

IT security professionals and leaders are too precious a resource to risk losing them to an overabundance of bad days in the office.

It should be noted that the results of this survey do not point to collapsing morale and an impending revolt. But what they do highlight is a growing sense of frustration, isolation, and annoyance – which in their combination is causing higher stress levels.

One thing that is certain however is the nature of the security threat, which only promises to grow in size and sophistication. Combatting this risk, and keeping organisations safe and sound, are objectives that rely heavily on motivated and empowered experts – and therein lies the rub.

It's a situation made easier when more good days are routinely experienced by IT teams.

As for the 'how', this report brings into focus the main causes of dissatisfaction. Some of these come with a seemingly quick and easy fix, such as the allocation of more skilled resource. A solution potentially easier said than done given the ever-widening skills gap. Other challenges can appear to require a longer-term answer. The need to better align desired organisational outcomes with the needs of tight IT security being a case in point.

But this issue, as with the exasperation noted on the topic of monotonous activity, can be addressed effectively only once IT teams are able to focus more attention on those aspects of their role designated as 'strategic'.

That's why the most comprehensive solution for the long-term is a transformation of your SecOps, in terms of delivering progressive change to the technology, processes, team structures, and people involved. Where the emphasis is placed on implementing an end-to-end platform approach to security. Supported by automation and orchestration capabilities that are trusted to perform the lion's share of recurrent tasks, thereby freeing up your staff to learn, strategise, and improve. An outcome based on modern security tools that help your business navigate today's threat landscape in a highly modern way.

Which sounds like a good day in anyone's book.

About this survey

This survey was carried out by Savanta on behalf of CAE Technology Services Ltd.

- A survey of 204 people in the IT industry, split between IT leaders (53%) and IT professionals (47%)
- A good spread of industry sectors was achieved, including representation from financial services (25%), professional services (31%), retail & distribution (16%), manufacturing (12%), and government (12%)
- All respondents were working in organisations where the IT function supports between 250 and 2499 users

As for CAE, we operate to a guiding purpose of transforming people's experiences and people's lives through technology. Our goal is to help inspire more good days at work, which we do through the delivery of intuitive IT services that make people's lives more straightforward, productive, fulfilling, and enjoyable.

This is technology that's on point, and aligned to the way different individuals and teams want to use it.

To engage with CAE is to enjoy the support of trusted experts able to advise you on what's needed to create and sustain practical value. The people you can turn to for tried and tested support when employees are not having a good day, getting them back on track as quickly as possible.

These are outcomes we achieve by working closely with clients to understand the exact stage reached on their IT journey, and the destination they're heading towards – then doing what's needed to achieve the desired end state.

A commitment we sum up in a simple ambition: more good days.

CISCO Partner

This report was produced in association with Cisco

Inspire your people to have more good days

If this report has got you thinking and wanting more good days for your people, including those legends in the IT team, then CAE could prove to be an ideal call.

You can take a look at our headline offerings spanning security, networks, cloud, data centre, workplace, and connectivity at **thisiscae.com**. Or if you want to talk through an idea or how we can help with the current priority list, then get in touch:

0845 643 0033
hello@thisiscae.com
thisiscae.com

CAE
TECHNOLOGY ON POINT