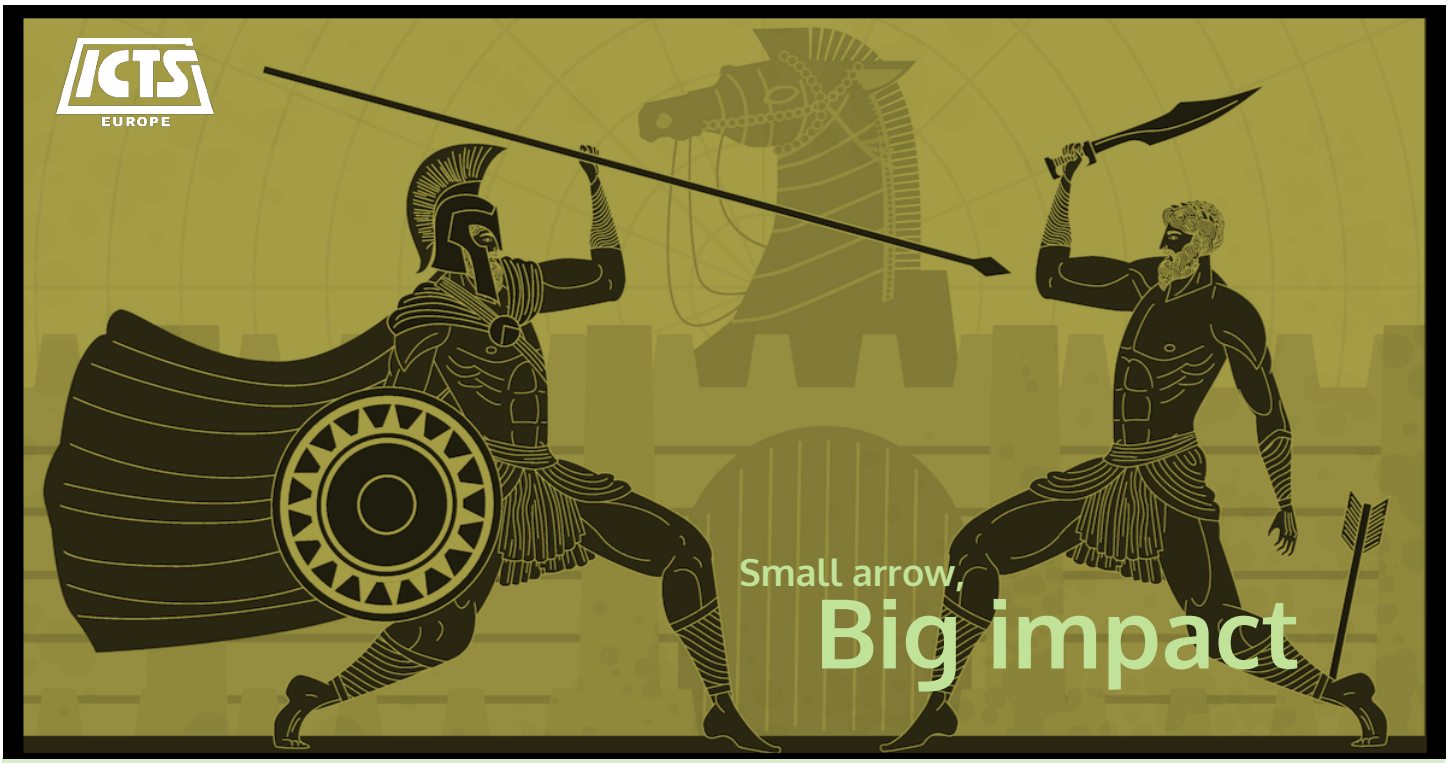



# STAFFING DATA CENTRES MAY EXPOSE AN ACHILLES' HEEL

**In our third 'fresh look at Heroes and Legends', Achilles reminds us why our perception of risk and vulnerabilities should be kept candid *and* current.**

Of all the myths and symbolism originating from Homer's epic poem and accounts of the Trojan War, Achilles is one of the most familiar characters and most frequently cited today – albeit as a cautionary tale.

Considered invulnerable and invincible, Achilles was not only an icon of superhuman strength and courage - but he was also on first name terms with the Gods. Despite having all the attributes of a hero, a single shot guided by luck, skill, or divine intervention made his name synonymous with hidden weakness and downfall.

Achilles' belief in his invulnerability blinded him to danger and relaxed his guard against anything less than a full-on attack.

Given enough time, determined adversaries will identify potential weaknesses and try to exploit them - from a safe distance if possible. Achilles was no exception; it was simply a matter of time, anatomy and ankles.

As a cautionary tale, it doesn't take a security professional to grasp the importance of searching for potential vulnerabilities and mitigating them. Data centre security specialists may also draw parallels from the high-impact nature of the attack: a single shot, directed at an unexpected but critical point of failure, causing a cascade of unrecoverable damage.

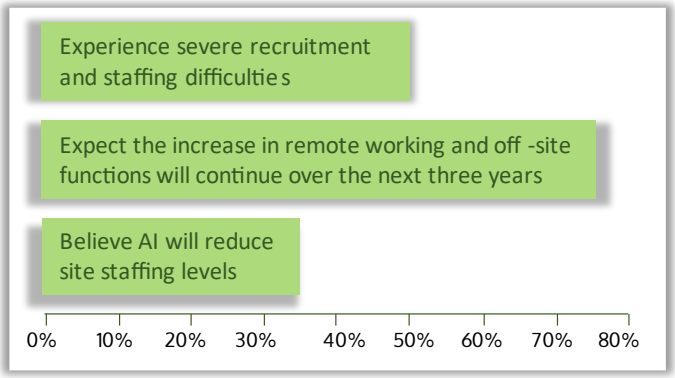
Now, more than ever, data centres have good reasons to re-evaluate their vulnerabilities and risks within the context of current sector trends.

## STAFFING: THE NEXT BIG CHALLENGE

Data centres face a significant staffing challenge as rapid infrastructure expansion increases the demand for skilled staff. The Uptime Institute's recent Global Staffing Forecast estimates that the Sector will need to fill 300,000 new vacancies by 2025.

This challenge is made more complex following eighteen months of lockdown, furlough, and working from home, which has drained the pool of job seekers in Europe and North America,

As it stands, 50% of surveyed Data Centres reported *Severe Recruitment Difficulties* in 2020.




Also apparent in the report is how data centres are preparing to solve this problem. Unsurprisingly, many Operators are seeking solutions that require less presence on-site and aim to reduce headcount.

The report concludes that data centres will likely become smarter, darker, and emptier as effort and funds are focused mainly on developing specialised technologies that support automation, remote system access, off-site monitoring, and multi-skilling.

## WHAT ARE THE CHALLENGES OF SECURING A SMARTER, DARKER AND EMPTIER DATA CENTRE?

ICTS Europe believes this question warrants the consideration of all data centre operators and one that service providers should be ready to answer. We take pride in being the go-to security partner to organisations where security failure is not an option. Our data centre clients trust us to provide fail-safe security solutions. They also expect us to help them identify new risks trends and work in partnership to develop their unique strengths.

As more data centre roles such as business support, system technicians, and management team functions move away from on-site work models, their physical security teams will continue to represent a *constant* presence on-site.

With a diminished opportunity for supervising routine activities through physical proximity, new, enhanced safeguards will be necessary to prevent a creeping erosion of professional standards or vigilance.

Critically, an effective incident response will have to balance the increased reliance of on-site teams to react quickly and independently to any issue while adhering to approved operating protocols.

The emerging paradigm for reduced headcount data centre operations hinges on unsupervised tasks being carried out correctly, maintaining standards, and individuals making the right decisions and taking the right actions. However, although 'erring' may be human, as much as 79% of data centre outages could be attributed to human error, according to the recent Uptime Institute Global Data Centre Survey 2021.

Essentially, anyone who has access to or influence over a system has the potential to become its 'Achilles Heel', however inadvertently.

## HOW CAN WE MINIMISE THE PROBABILITY AND IMPACT OF HUMAN ERROR?

reTo answer this question, we must consider one of the most common causes which lead to mistakes, which is critical but controllable, '*state of mind'.* People make more mistakes when they feel excessive pressure, fatigue, distraction, fear of failure, and judgment.

It may also be helpful to understand the two systems people use to make decisions and act:

1. **Intuition:** automatic, emotive response with limited information processing; fast and low effort.
2. **Analysis:** rational response, based on processing knowledge and information; slow and high effort.

Intuition is considered the primary method people use to make decisions and define actions. Our brains have developed an innate bias for automation to conserve energy, particularly when inactive or engaged in repetitive tasks over extended periods. Unfortunately, in this mode, mistakes increase. Once our brain switches to auto-pilot, it is only a matter of time.

People can, however, switch to analysis mode, override intuitive decisions and improve their ability to make 'the right call'. Three essential ingredients are required:

1. Possessing adequate experience and knowledge
2. Clear and relevant information to allow proper understanding of the situation
3. An optimal state of mind, free of the premonitions mentioned earlier.

## DODGING THE ARROW

Thankfully, data centre security professionals can avoid repeating Achilles' mistakes. Data centres are developing technologies to mitigate staffing shortfalls and facilitate safer, more efficient off-site work operations. As their physical security teams will continue to provide on-site protection, they must also be equipped with the expertise and solutions to reflect their increased isolation and independence.

*'A man's acts follow him wherever he goes',* wrote David Malouf on Achilles.

We believe that *successful* acts are more likely to follow when committed security personnel are equipped with bespoke, meaningful, data-driven tools that increase productivity, boost performance, and enable them to work smarter and faster rather than longer.


Garry.Malone@ictseurope.com www.ictseurope.com