WHEN FAILURE IS NOT AN OPTION

WHAT DO DATA CENTRES, WILHELM TELL AND APOLLO 13 HAVE IN COMMON?

On the virtues of preparedness and precision:

Who isn't familiar with the story of Wilhelm Tell and the apple shot? As the tale goes, the Swiss folklore hero, having refused to bow before an evil Vogt, was given a terrible choice: execution, or with one shot from his crossbow, split an apple placed on his son's head, 100 meters away. The thought of finding yourself in Tell's pointy leather shoes is enough to make your toes curl in dread.

Many believe that Wilhelm Tell was a real person, not just a fictional construct; that all of this took place one autumn day in 1307 – one of many audacious exploits that generations of proud Swiss ascribe to the expert marksman.

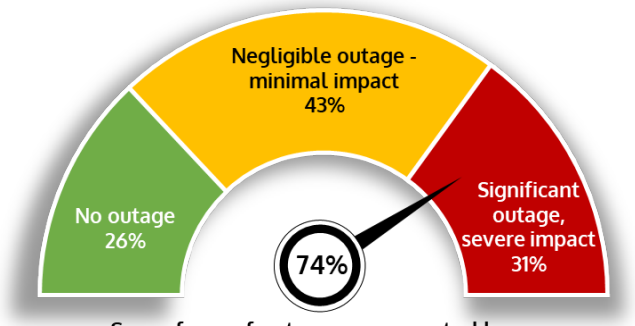
Mr Tell (and his son) lived to tell the tale, and many more besides. But none have endured so well or resonated as universally as the apple shot. And why not? It is a tale of courage in the face of tyranny, skill and canny – and it comes with a happy(ish) ending. It inspired a nation to rebel and was repeated in countless poems, plays, music and movies.

Still, amidst the lauding of the celebrated shot, lest we neglect the moments just before the bolt was launched. Imagine what goes through the archer's head as he fixes his sights on the apple, gauging the wind, praying the boy doesn't move. So much is at stake; so many things can go wrong.

When you can't afford to fail, how do you develop the skills and tools necessary to ensure that you get it right?

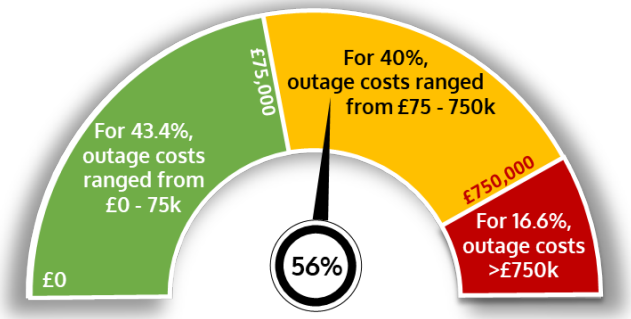
ICTS Europe has been asking these questions for thirty years, and we are still coming up with new answers. We take pride in being the go-to security partner to organisations where security failure is not an option. High-risk, global organisations trust us with their business and their customers. In addition to securing assets, reputation, life and limb, we safeguard Bits and Bytes for data centres that view security as a critical success component.

For data centre operators, outage is the ultimate risk. Despite steady improvements in infrastructure and practice, outages remain a significant concern. A recent Uptime Institute survey reports that 44% of data centre operators are more concerned about outages now than they were one year ago. Indeed, 74% of surveyed data centres experienced some form of outage during 2020. Crucially, three out of ten experienced outages with significant or higher impact.



Some form of outage was reported by almost ¾ of data centres surveyed in 2020

The precise impact of outages is hard to measure because most outage incidents are not reported. As seen below, according to surveyed data centres operators, only 16% of outage incidents in 2020 carried a total price tag above £750k.



More than half of the data centre outage costs reported in 2020 exceeded £75k

However, research by Statista suggests that in 39% of cases, the collateral cost of one-hour outage/downtime is $1 million or more, while the most common events cost $300k - $400k for each downtime hour.

While the industry finds it hard to agree on calculating impact, there is a standard agreement on the causes of outage and downtime. In the past, the most common culprit was technical failures - mainly of power supply and switching systems. In recent years, outages are increasingly caused by misconfigured IT and network systems. There is general agreement that cybercrime is rapidly becoming a prevalent threat to uptime.

Human error also continues to play its part in most outages. As much as 75% of significant downtime incidents were caused by human error that could have been avoided with better management or processes, according to respondents of the Uptime Institute's Annual Survey, 2020. With cybercrime threats on the increase, reducing the probability of human error becomes an absolute priority.

How would these notions help us in constructing a fail-safe approach to delivering optimal security to data centres? This is where Apollo 13 comes into play. Long before 'failure is not an option' became a catch-phrase for the 1995 Apollo 13 movie, it was the underlying credo of NASA's missions. Many studies have been undertaken to identify the key elements of NASA's approach to fail-safe planning and execution.

Typically, *teamwork* and *leadership* occupy the top spots on the list. *Diversity of skills and expertise* is another key ingredient, as is the ability to *assimilate lessons and experience quickly*. But **the most vital component of critical failure avoidance is Situational Awareness**.

In NASA's research paper *Intelligent Automation Approach for Improving Situational Awareness,* three levels of awareness and impact are identified:

BASIC: Relevant information presented in a manner that allows full appreciation of the state of critical systems and processes.

HIGH: Understanding of critical systems and processes status directs the correct action of immediate tasks.

ULTIMATE: Use of high-level Situational Awareness to anticipate future events and direct failure-preventing perception and actions.

This is a powerful blueprint for delivering optimal security to data centres. Ultimate situational awareness enables us to work today to reduce the probability and impact of outages in the future. It does not negate the need for a Plan B but reduces the likelihood of deploying such resilience measures.

This leads us back to our hero – who also had a Plan B. when preparing for his 'single shot', he took two bolts from the quiver. Moments later, apple pinned to tree and son unharmed, Tell was asked what the second arrow was for?...

We leave our readers to guess (or Google) Tell's reply which turns his story into one of resilience; a topic so critical, it deserves individual attention or an article of its own.

Watch this space!

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