Masters of Machines III: Mitigating the Impact of Critical IT Events

A critical IT event (CIE) occurs when a business application or infrastructure is down, or has a malfunction, whereby a business process is halted, or users are unable to reasonably carry out tasks and transactions.

DOWNTIME TRUMPS SECURITY

For the first time, downtime has replaced security as the top concern for IT management.

The overlap in use of on-premises and cloud services implied by these figures shows that hybrid deployment is now near ubiquitous.

Whilst there are many benefits to be had from hybrid IT deployments, it contributes to complexity and may lead to increased downtime.

86% of organisations use software-as-a-service
80% of organisations use infrastructure-as-a-service
94% still use on-premises servers for primary or secondary IT deployment

THE COST OF CIEs

The average number of CIEs per European organisation per month is 3. 65% of European organisations report that a past CIE has led to reputational damage and associated financial losses.

THE IMPACT OF IT OPERATIONAL INTELLIGENCE ON RESPONDING TO CIEs

IT operational intelligence is the ability an organisation has to gain insight into events that occur across its IT infrastructure.

CIE TEAMS PRODUCTIVITY

VISIBILITY AND RCA

The cost per team member per CIE can be reduced by 25% through effective operational intelligence.

Those that collect the most machine data have a better operational intelligence capability.

IT operational intelligence is the ability an organisation has to gain insight into events that occur across its IT infrastructure.

MAP OF RESPONDENTS

Try our critical IT events calculator at ciecalculator.com

Source: Master of Machines III - Mitigating the impact of critical IT events