Could hidden OT security gaps be putting your Data Centre at risk?

oryx
align

When OT systems go unpatched, risk builds fast

85%

of organisations don’t regularly patch OT systems due to fears of operational disruption.

37% of OT breaches stem from already disclosed vulnerabilities.

Security breaches are no longer just an IT problem

10%

of data centre outages are now caused by cybersecurity breaches.

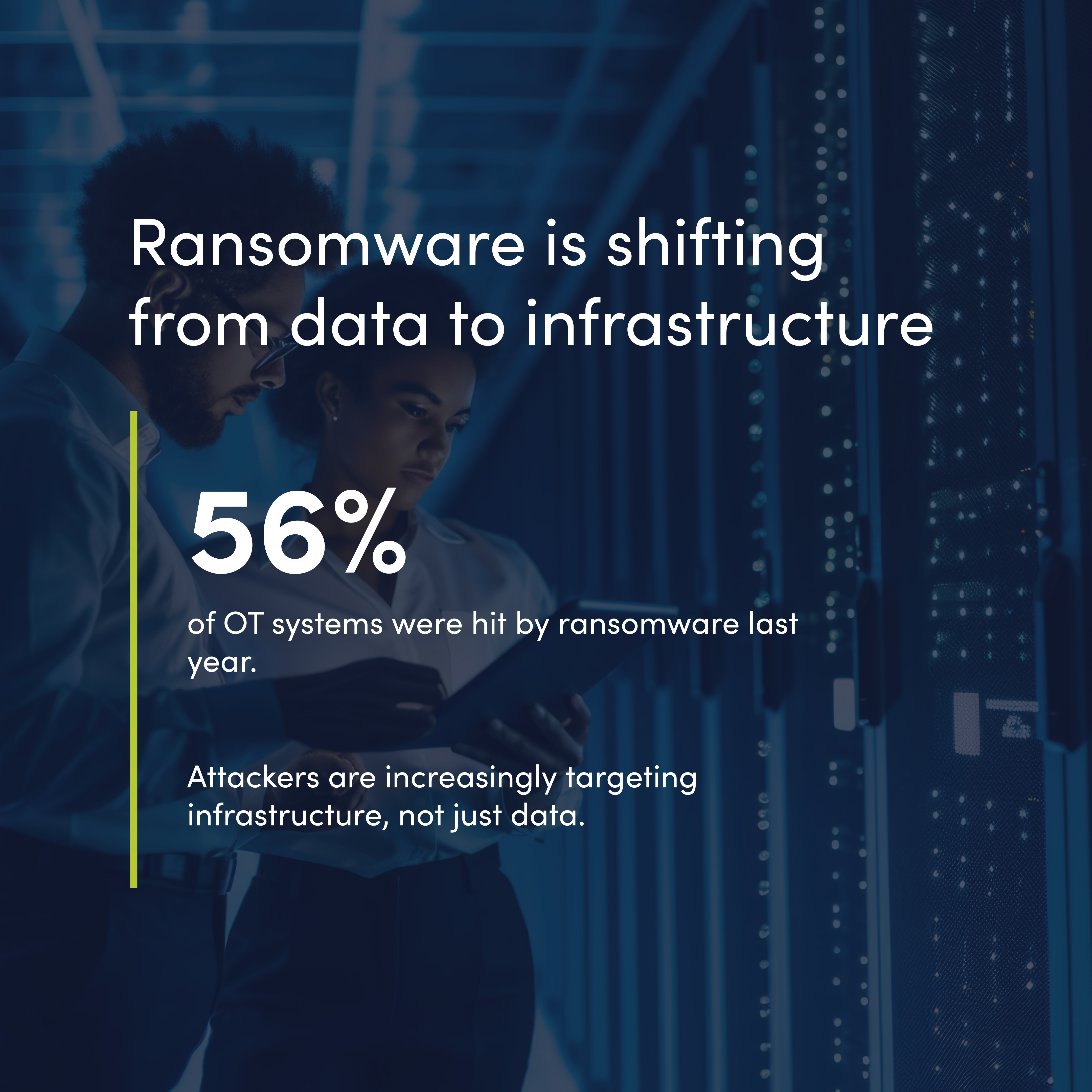
The financial impact of a single hour of downtime can exceed £1,000 per megawatt (MW), not including reputational damage.

Misconfigured systems are easy targets for attackers

70,000

OT devices (like SCADA controllers and HMIs) are directly accessible online.

Most of these devices run outdated or vulnerable firmware, making them easy targets.



Ransomware is shifting from data to infrastructure

56%

of OT systems were hit by ransomware last year.

Attackers are increasingly targeting infrastructure, not just data.

OT security can't be left to chance

As IT, OT and IoT converge, security must keep pace

Find out how to secure every layer of your data centre:

oryxalign.com/data-centre

oryx
align