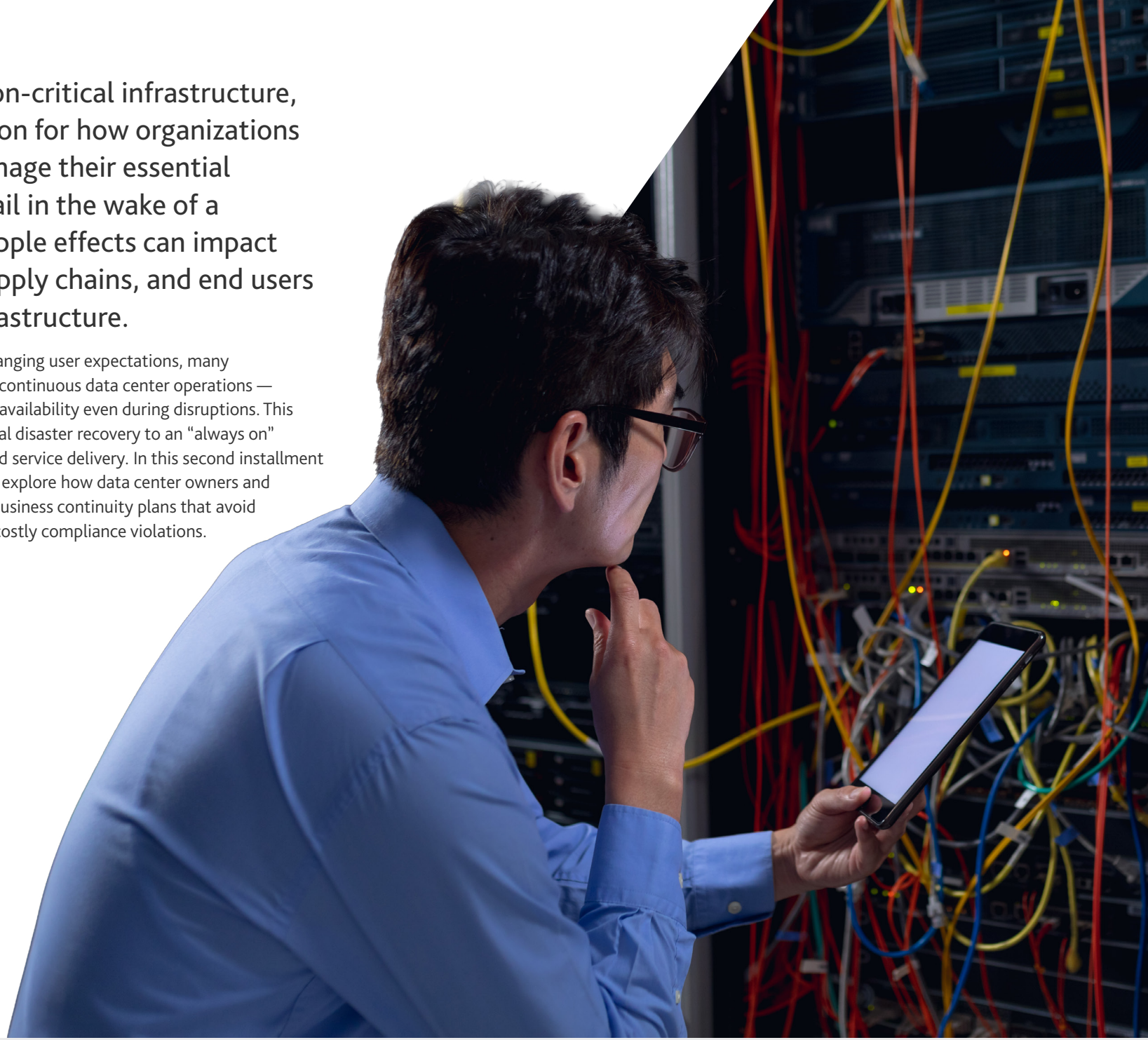
Data Center Dangers:

Building Resilient Business Continuity Plans for Critical Infrastructure

BDO

Data centers are mission-critical infrastructure, serving as the foundation for how organizations store, process, and manage their essential system. If operations fail in the wake of a disruptive event, the ripple effects can impact dependent services, supply chains, and end users who rely on digital infrastructure.

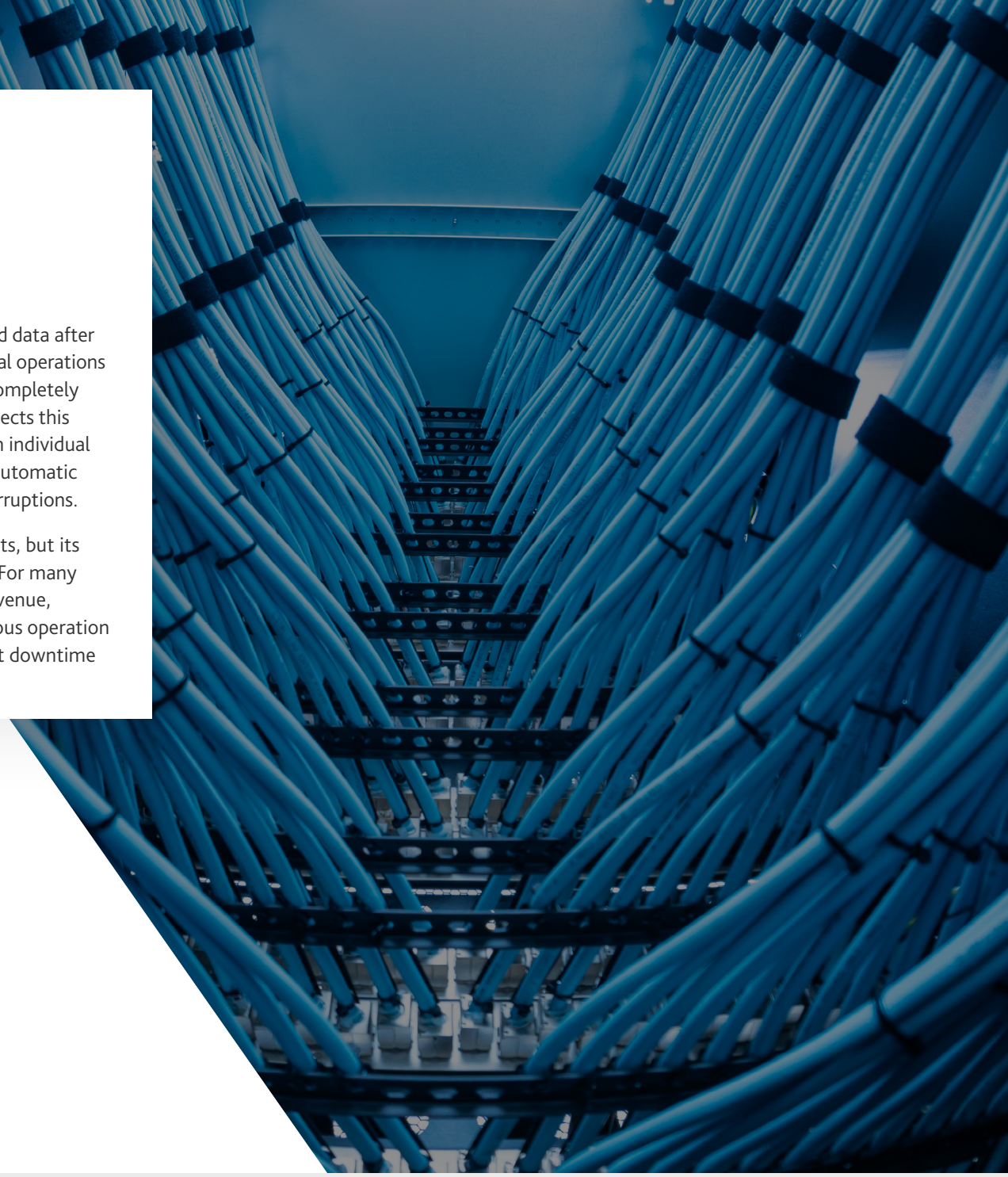
To prevent interruptions and meet changing user expectations, many organizations are seeking to establish continuous data center operations — systems designed to maintain service availability even during disruptions. This focus represents a shift from traditional disaster recovery to an "always on" approach that prioritizes uninterrupted service delivery. In this second installment of our Data Center Dangers series, we explore how data center owners and developers can build comprehensive business continuity plans that avoid detrimental down time and mitigate costly compliance violations.



Beyond Traditional Diasaster Recovery

Traditional disaster recovery concentrates on restoring IT systems and data after an incident, while business continuity focuses on maintaining essential operations during a disruption. Disaster recovery accepts that systems will fail completely and measures success by restoration speed. Continuous operation rejects this premise, instead prioritizing systems that maintain service even when individual components fail through mechanisms like redundant pathways and automatic failover capabilities that activate before users experience service interruptions.

Traditional disaster recovery does require smaller upfront investments, but its true price also includes the cost of downtime when incidents occur. For many organizations, even short outages can translate to millions in lost revenue, damaged customer relationships, and regulatory penalties. Continuous operation models demand higher initial capital expenditure but eliminate most downtime costs by embracing prevention over reaction.



Modern Continuity Challenges

Continuous operations are an appealing prospect, but modern artificial intelligence (AI) workloads can make implementation challenging. AI data centers require sustained computational power across distributed systems, making brief interruptions as damaging as extended outages. Unlike traditional applications that can tolerate short service gaps, AI needs continuous processing to maintain model accuracy and real-time decision-making capabilities.

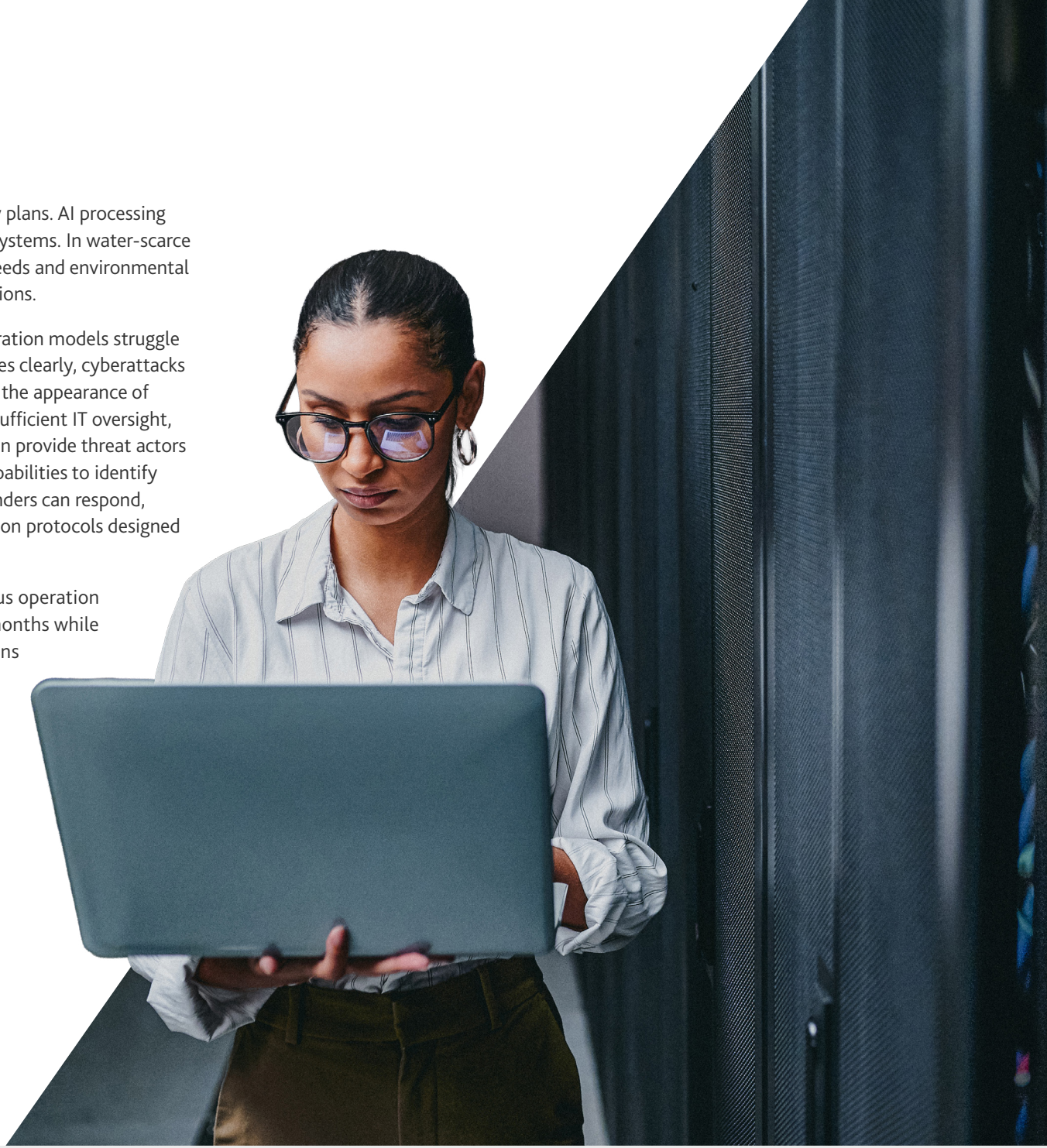
Organizations are responding to these power constraints by clustering data centers to distribute processing loads in the event of an outage, as well as exploring co-location strategies that provide geographic redundancy without sacrificing performance. This distributed approach can help ensure sufficient capacity are in place, but it also brings new infrastructure demands that continuous operation planning fails to address.

Power infrastructure represents the most immediate threat to a continuous operation model. Regional power grids struggle with AI workloads, which consume exponentially more electricity than conventional computing tasks. Many regions also implement planned power shutdowns during extreme weather conditions, forcing data centers to operate on backup systems for extended periods. But traditional backup options often fall short. Generators designed for brief outages cannot keep up with demand, while renewable sources like solar and wind do not always provide consistent power generation.

Water consumption creates another pressure point for continuity plans. AI processing generates substantial heat loads that rely on aggressive cooling systems. In water-scarce regions, this reliance can lead to conflicts between data center needs and environmental regulations, forcing operational reductions during drought conditions.

AI workloads also increase data breach risks that continuous operation models struggle to address. Unlike infrastructure failures that announce themselves clearly, cyberattacks often establish hidden footholds with systems while maintaining the appearance of normal operations. If companies deploy AI applications without sufficient IT oversight, they open the door for **unmonitored "shadow" AI usage** that can provide threat actors with attractive entry paths. Once inside, attackers leverage AI capabilities to identify vulnerabilities and adapt their strategies faster than human defenders can respond, compromising multiple network segments while avoiding detection protocols designed to avert human-led intrusions.

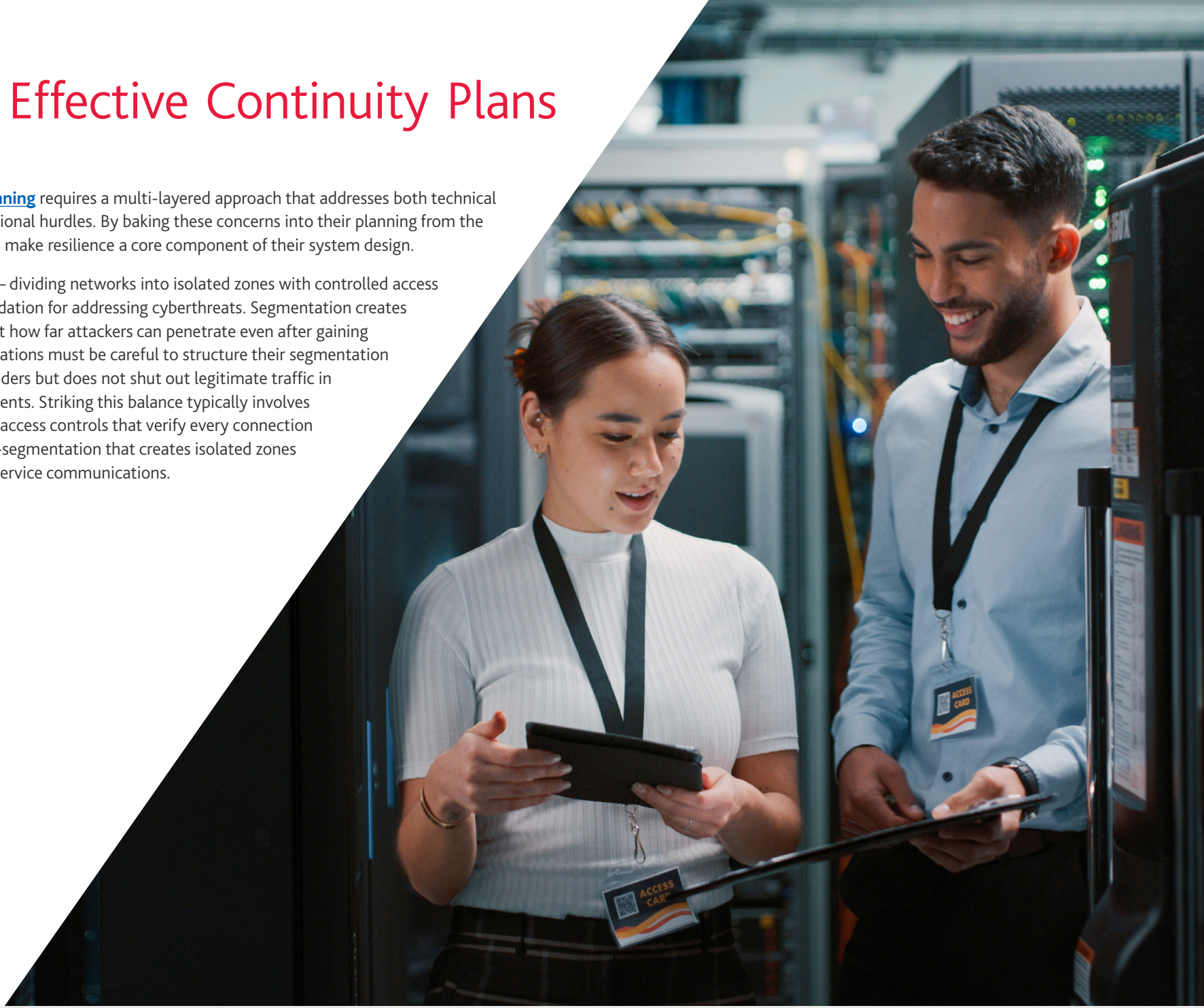
The persistence of these threats creates a paradox for continuous operation models. Successful data breaches can operate undetected for months while threat actors map networks and extract data. When organizations discover these intrusions, the scope of compromise often requires some form of system replacement to ensure the threat is eliminated, forcing organizations to choose between uninterrupted service and verifiable security.



Building Effective Continuity Plans

Effective **continuity planning** requires a multi-layered approach that addresses both technical infrastructure and operational hurdles. By baking these concerns into their planning from the get-go, organizations can make resilience a core component of their system design.

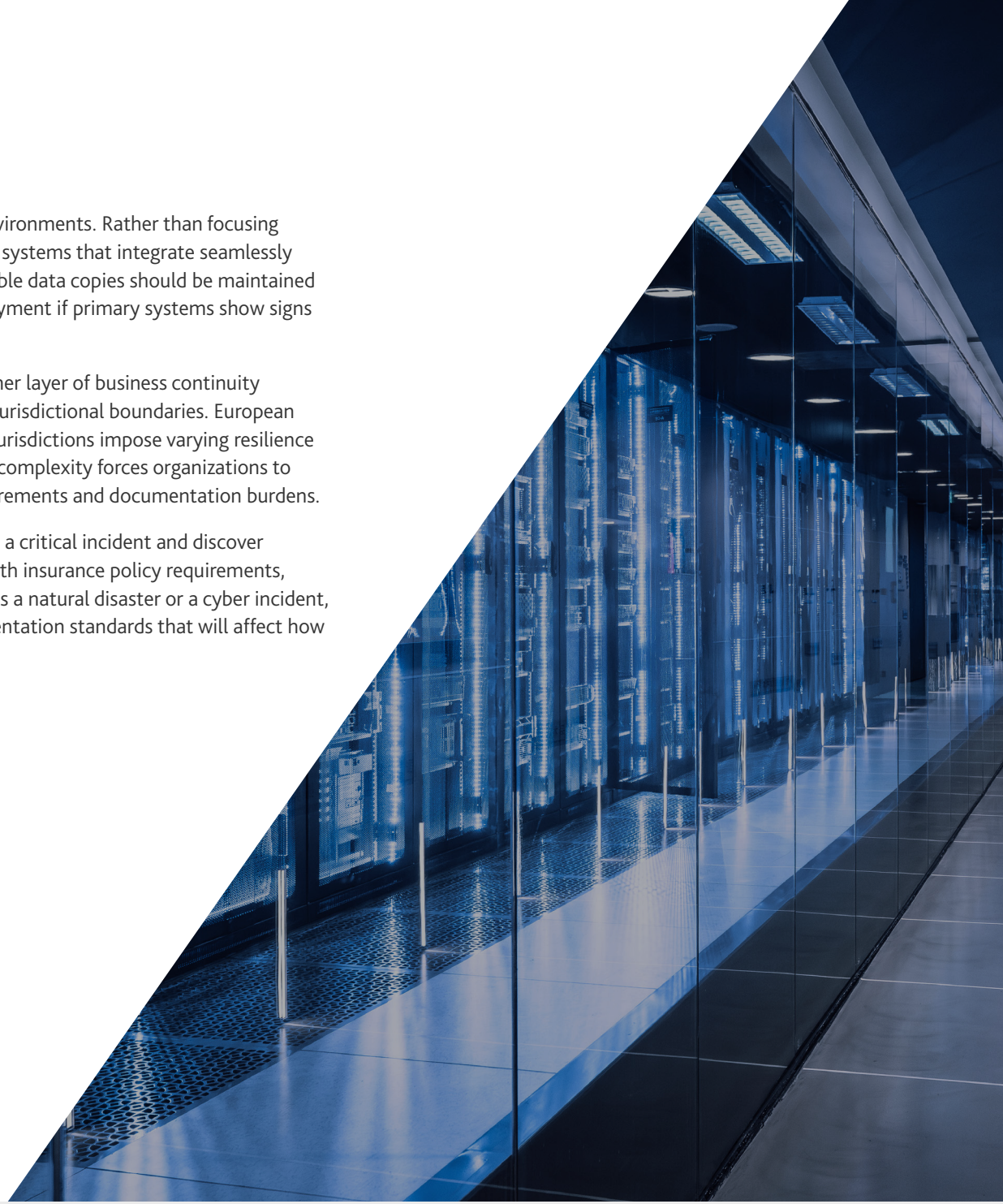
Network segmentation — dividing networks into isolated zones with controlled access points — is a strong foundation for addressing cyberthreats. Segmentation creates internal barriers that limit how far attackers can penetrate even after gaining initial access. But organizations must be careful to structure their segmentation in a way that blocks intruders but does not shut out legitimate traffic in live production environments. Striking this balance typically involves implementing zero-trust access controls that verify every connection request, as well as micro-segmentation that creates isolated zones while preserving critical service communications.



Air-gapped backups can also make a significant difference in "always on" environments. Rather than focusing solely on data recovery after system restoration, organizations need backup systems that integrate seamlessly into active operations without requiring extended retrieval periods. Immutable data copies should be maintained in highly secure, offline environments that remain accessible for rapid deployment if primary systems show signs of an intrusion.

Distributing systems across multiple availability zones can provide yet another layer of business continuity protection, but it may also introduce compliance challenges if data crosses jurisdictional boundaries. European markets mandate specific **operational resilience capabilities**, while other jurisdictions impose varying resilience standards that organizations must navigate simultaneously. This regulatory complexity forces organizations to weigh the benefits of geographic redundancy against data sovereignty requirements and documentation burdens.

Finally, organizations often overlook **insurance coordination** until they face a critical incident and discover coverage gaps. Effective business continuity planning should always align with insurance policy requirements, which differ significantly depending on the source of an event — whether it is a natural disaster or a cyber incident, for example. Many policies call for specific response procedures and documentation standards that will affect how organizations execute their continuous operation strategies.



Proactive Versus Reactive Planning

Organizations that fail to engage in continuity planning before a disaster strikes will be stuck paying a premium for emergency services, extended recovery periods, and reputational damage that persists long after the core technical issues are resolved. Increased regulatory attention, which often follows major incidents, can compound these issues. It may result in extended oversight, mandatory reporting requirements, and penalties that create ongoing operational constraints.

Businesses that embed continuity planning into their initial data center design process can better identify vulnerabilities and implement **risk mitigation** tactics before they cause harm. A proactive approach is cheaper than reactive solutions and can provide superior protection, since continuity measures work most effectively when integrated into fundamental system architectures. That said, organizations must maintain robust traditional disaster recovery capabilities in addition to continuous operations. Even well-designed resilient systems can fail, and in dynamic environments, hidden connections between systems often amplify outage impacts in unforeseen ways.

Once implemented, effective continuity programs require ongoing iteration. Threat landscapes change rapidly, regulatory requirements expand regularly, and operational needs shift as organizations grow and adopt new technologies. Regular testing through tabletop exercises and simulated incidents often exposes coordination problems, communication failures, and resource constraints that an organization's original plans have overlooked.

Final Thoughts

The ongoing shift from disaster recovery to continuous operations represents more than a technical upgrade. It heralds fundamental changes in how organizations approach risk management, operational planning, and incident response.

BDO can help organizations navigate this shift and address pressing challenges across the continuity spectrum. From immediate incident response and reputation management during crises to post-incident analysis and future prevention strategies, our experienced teams can help position your organization to maintain operational effectiveness when disruptions inevitably occur.

CONTACT US

TOM MANNION
National Data Centers Practice Leader
tmannion@bdo.com

STEVE TAYLOR
Director, Forensics
setaylor@bdo.com

MATT GROSSMAN
Director, Forensics
mgrossman@bdo.com

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.