Data Center Dangers:

Addressing Digital, Physical, and Environmental Security Threats

BDO

Data centers serve as the backbone of modern digital operations, powering everything from financial transactions and healthcare systems to cloud computing and artificial intelligence (AI). Due to their critical importance, these facilities face an evolving array of security threats that, if left unaddressed, can cause disruptions across society. In the first article of our Data Center Dangers series, we explore the different kinds of security threats facing data centers and how best to protect against them.

The Evolving Threat Landscape

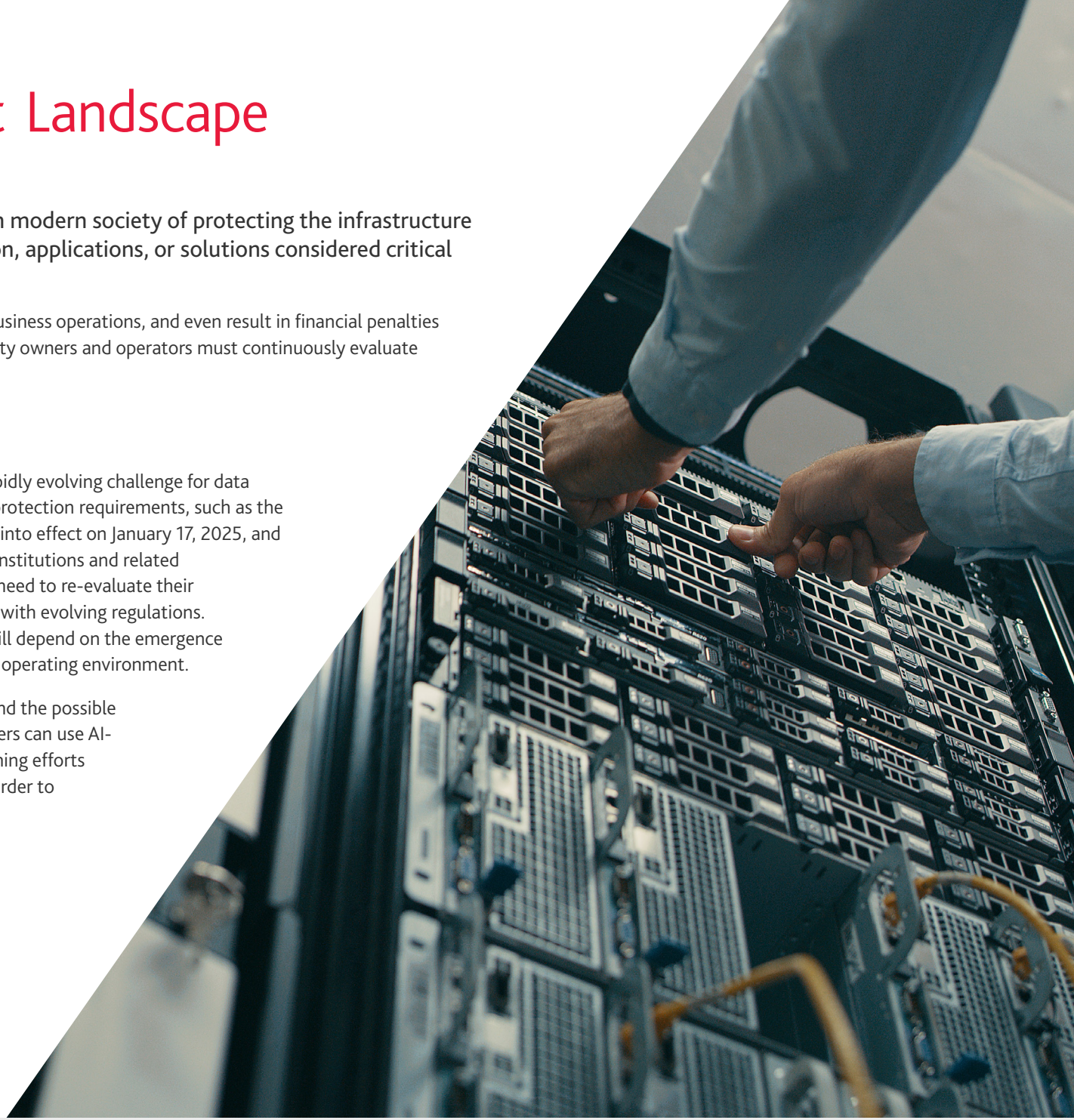
Data centers play an increasingly integral role in modern society of protecting the infrastructure they house, which may include data, information, applications, or solutions considered critical to their customer(s).

A single security breach can damage client trust, disrupt business operations, and even result in financial penalties or regulatory action. As the threat landscape evolves, facility owners and operators must continuously evaluate their security protections.

DIGITAL THREATS

The digital threat landscape presents perhaps the most rapidly evolving challenge for data centers. New regulations are expanding data privacy and protection requirements, such as the **Digital Operational Resilience Act (DORA)**, which went into effect on January 17, 2025, and introduced new compliance requirements for all financial institutions and related technology providers working in the EU. Data centers will need to re-evaluate their compliance programs on a regular basis to stay up to date with evolving regulations. The frequency of re-evaluating the compliance program will depend on the emergence of new threats and how often the company is changing its operating environment.

Another threat to consider pertains to privacy standards and the possible impact from sophisticated AI-powered cyberattacks. Hackers can use AI-generated executive voices, for example, to make their vishing efforts seem more realistic. These AI-enabled threats are much harder to detect and prevent than traditional attacks.



PHYSICAL SECURITY THREATS

Despite robust physical barriers including vehicle blockades, cage systems, and specially designed door hinges, unauthorized access to data center premises remains a risk. This challenge is greater for colocation arrangements in which multiple companies share a facility, expanding access points and vulnerabilities. To prevent unauthorized entry, facility owners need to conduct regular physical security assessments and consider changes to controls based on new emerging threats.

Hardware disposal presents another physical security concern. When maintenance contracts include hard drive replacement, wiping confidential data requires proper certification and chain-of-custody documentation. If the data center fails to fully wipe the data, it risks potentially exposing sensitive client information.

ENVIRONMENTAL AND INFRASTRUCTURE THREATS

Data center safety is highly dependent on location. During the **site selection process**, data center owners should carefully consider environmental risk factors, such as insurance premiums and proximity to flood zones.

Infrastructure design decisions also play a crucial role in security. For example, facilities need to be designed for fire prevention and leverage sophisticated fire detection and monitoring tools. Key design elements that need to be taken into consideration include implementation of fire-rated walls, subfloor compartments, and monitoring and detection of the infrastructure for overheating.

Early detection and notification are key for colocation providers where downtime can impact multiple companies. Traditional water sprinklers are not suitable for today's data centers — rather, clean agent fire suppression systems using agents such as FM-200, Novec 1230, or Inergen are used to better protect sensitive equipment and maintain safety standards.

Data centers also require tremendous amounts of energy to function, and the unreliability of the power grid poses one of the biggest risks to both operations and security. Plugging directly into renewable energy assets with a "behind-the-meter" configuration can help data centers address this risk by offering greater reliability and lower energy costs. Similarly, data center owners need to plan around maintaining access to water to cool systems and the costs of associated water usage.

Addressing Security Threats with Customers

To attract and retain customers, data centers need to prove the strength of their security programs. Different customers will have different expectations around how data centers should demonstrate their security positioning.

More established clients typically require security certifications or formal attestation reports, whereas some clients may not know what specific documentation they will need for their audits. Customers in highly regulated industries might require additional documentation to illustrate that their vendors are complying with specific industry standards, such as HITECH and HIPAA in the healthcare space.

Third-party certifications and reports allow data centers to provide standardized documentation of their security and internal controls to all customers, rather than handling customer inquiries on a case-by-case basis. Without proper attestation, data centers may face hundreds of annual security questionnaires from clients, which can be both expensive and time-consuming.

Some formal attestation reports that data centers clients often request include SOC 1 and 2, both governed by the American Institute of Certified Public Accountants (AICPA). Data center clients with international operations may also request certifications like ISO 27001 and PCI DSS. Attestation reports and certifications are critical for data centers to meet compliance requirements and identify and address potential gaps in their existing security.

Final Thoughts

Establishing adequate security protections is not a one-and-done task. Data centers face significant digital, physical, and environmental risks and failure to adequately address these risks as they evolve can have serious implications for national security. Data center operators must continually evolve their programs to meet changing compliance requirements and customer needs in an increasingly complex threat environment.

Further Reading

Explore our content to learn more about attestation reports and how you can strengthen your security positioning:

- Why Attestation Services Are Becoming More Important to Tech
- How to Evolve Your Privacy & Data Protection Program Checklist
- Avoiding Common Third Party Attestation Pitfalls
- Global Privacy & Data Protection eBook

CONTACT US

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

BRENT HORAK
National Data Centers Practice Leader
bhorak@bdo.com

GREG SCHU
Managing Principal, Risk Advisory Services
gschu@bdo.com

BINITA PRADHAN
Principal, Third Party Attestation
bpradhan@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.