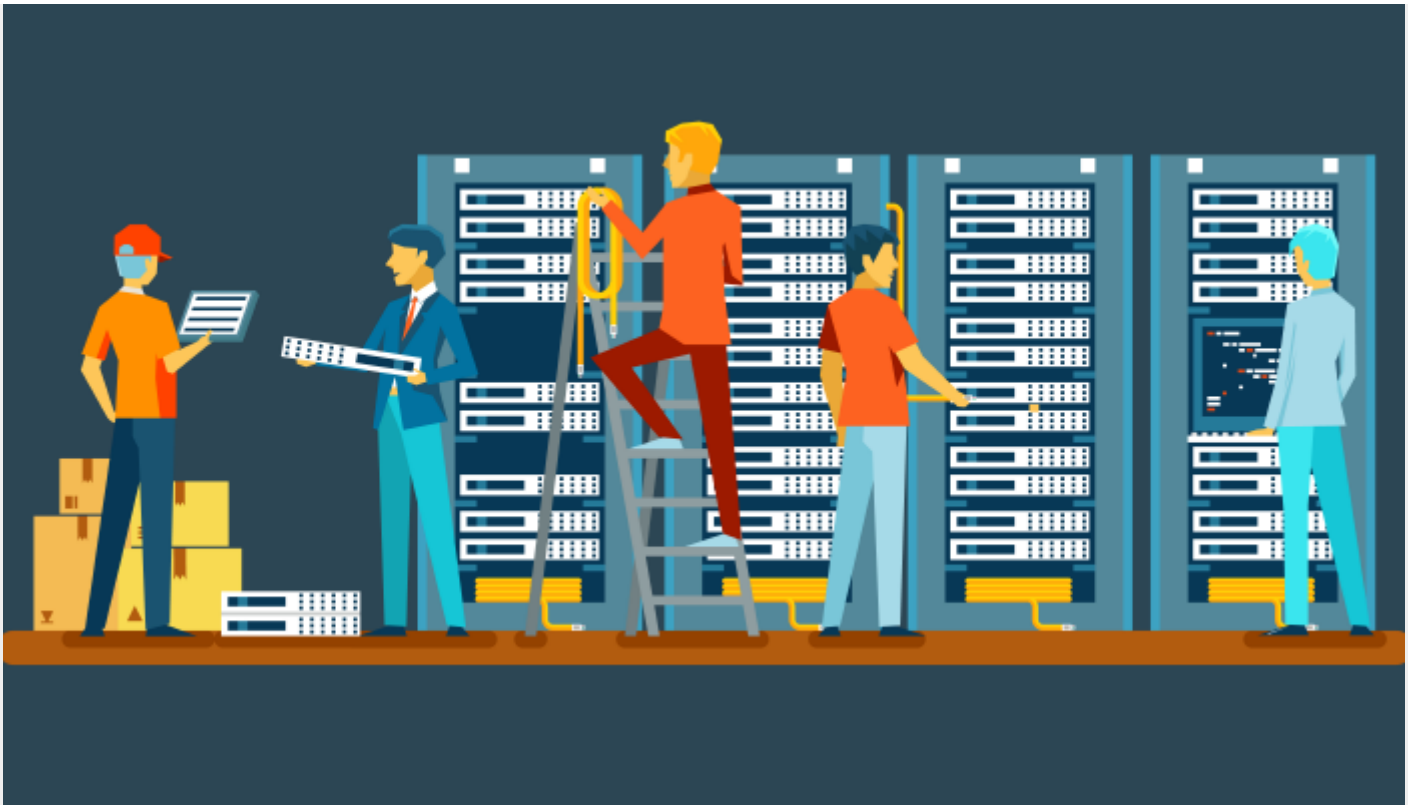
SECURING DATA CENTERS & SERVER ROOMS: GOALS & BEST PRACTICES

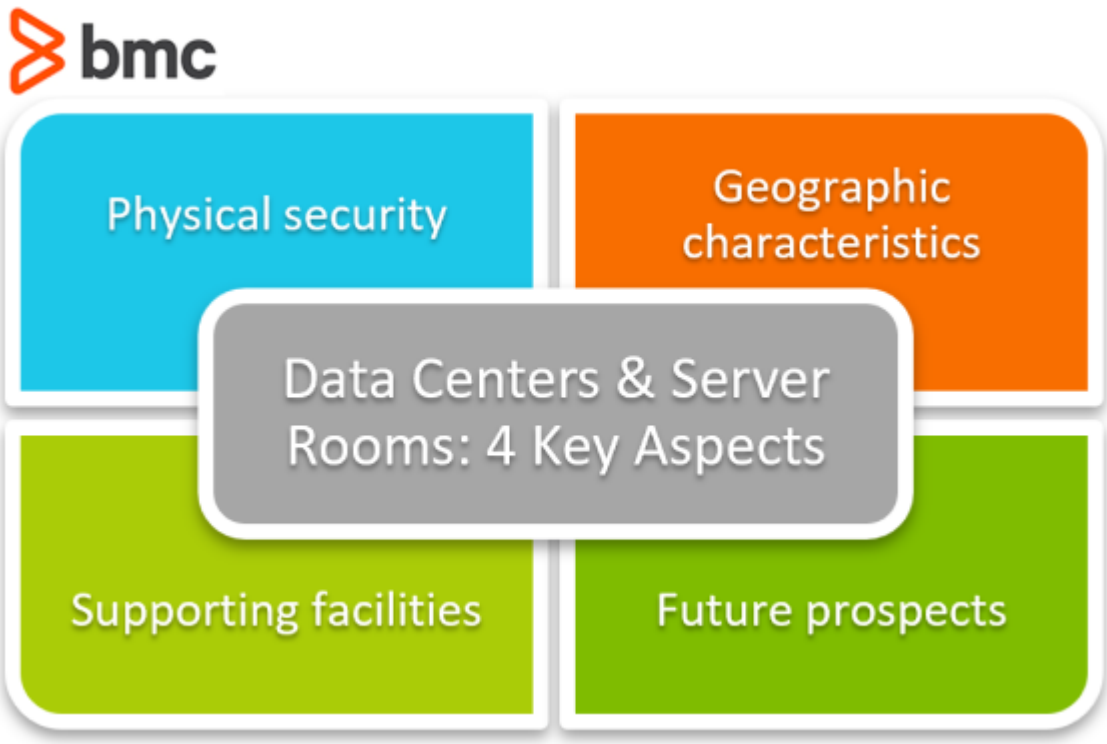


Information security is a critical topic in the enterprise IT industry, especially when mission-critical data is stored in cloud data centers off-premises. Indeed, cybercrime is the most pressing concern since 79% of the organizations using cloud computing services have experienced a cloud-related data breach incident according to a recent survey.

However, there's more to security of the cloud data center than defending against the prevalent cybercrime attack vectors. Physical security of hardware assets is equally critical for secure and dependable operations of a cloud data center.

In this blog, we will discuss what the physical security of a cloud data center entails, the applicable industry standards, and industry-proven best practices to secure your cloud data center resources.

(This article is part of our Data Center Operations Guide. Use the right-hand menu to navigate.)



Security controls for data centers & server rooms

Cloud data center and server room security controls encompass four key aspects of the data center:

- **Physical security.** The security of static systems that constitute a data center. The building structure, hardware resources, utility services infrastructure, as well as portable and mobile objects that constitute a data center facility are included. The characteristics of these systems determine the security and physical threats facing a data center including fire, unauthorized access, work conditions for the workforce, and dependability.
- **Geographic characteristics.** The location of a data center determines the natural threats such as earthquakes, flooding, and volcanic eruptions. Additionally, human-responsible threats such as burglary, civil disorders, interruptions, damages, and interceptions are also highly dependent on the location of the data center facility.
- **Supporting facilities.** Refers to the services necessary for smooth data center operations. These facilities include the infrastructure of utility services such as energy, water, cooling, communication, and air conditioning. Emergency services including firefighting, policing, and emergency healthcare also impact the risk mitigation capacity of a data center.
- **Future prospects.** Economic, political, geographic, and demographic factors affect how well a location is suitable for data center operations over the long term. The services and facilities available to your server room may suffice for now but does the location offer sufficient capacity, services, and facilities to scale in the future?

Securing your server room

The first step to securing a server room is to design one that is fully compliant to the leading industry standards. Organizations such as the National Institute of Standards and Technology (NIST) as well as government regulatory authorities provide guidelines, standards and frameworks that encompass all aspects of server room security: physical, environmental and information security.

Some of the common server room security standards and framework guidelines include:

- ISO 27001
- ISO 20000-1
- SSAE 18 SOC 1 Type II, SOC 2 Type II and SOC 3
- NIST SPs (including SP 800-14, SP 800-23, and SP 800-53)
- Department of Defense (DoD) Information Assurance Technical Framework

Server room best practices

Server room security is an ongoing process. The security frameworks provide guidelines to maintain server room security in context of changing external circumstances and the scale of IT operations. Once a data center room is designed in compliance with the applicable standards, the next steps involve a range of controls that can help mitigate threat vectors ranging from human risks to threats from natural disasters.

The following best practices and security controls can help you get started with data center security:

Restricted access & multi-layer authentication

Only the authorized personnel should be allowed to enter (and exit) the premises. Multiple layers of security—passwords, RFID tags, and biometrics—can be combined to enforce implementation.

Server systems should be isolated such that the principle of least privilege access can be adopted, ensuring that damage can be contained within isolated sections of the data center when compromised.

(Read about zero trust network access.)

Fire safety & HVAC

Fire incidents, explosions, and inadequate HVAC affect the dependability of a server room. These incidents can leave irreversible damages to a server room, especially when the stored data is not adequately duplicated. Consequently, it's important to evaluate the safety capacity of the building against these risks.

Adopt fire detection and control systems, automate emergency service routing and limit building occupancy. Data center efficiency is highly dependent on the HVAC systems. An effective server room design considers all aspects of ventilation, including damage limitation in event of a fire incident.

Building structure & utility infrastructure capacity

The hardware racks and building structure should be highly capable of supporting heavy hardware devices. Access to these devices should be convenient and systematic: troubleshooting, repairs, and upgrades should take minimal time and effort. The utility infrastructure that powers HVAC systems should be designed for:

- High capacity
- Structural integrity

- Long life

Information security

Physical security of a server room also impacts the ability to secure information stored within the server systems. If the data is encrypted, it will remain secure even when the storage devices in the server room are compromised.

Similarly, the server systems should be designed for redundancy. If one device is no longer operational or is compromised, the stored data should be accessible through alternative and redundant storage devices.

(Learn more about data center redundancies.)

Emergency services

In event of a security breach or emergency incident, access to emergency services—police, healthcare, and firefighting services—should be automated and highly available. Deploy automated technology systems to inform the appropriate emergency services in event of an incident and engage with private security services to enhance building security.

Securing server rooms is critical business

Securing server rooms is an absolute necessity. It is not a cheap endeavor (would you want cheap security?), so you'll have to find some custom balance of security, accessibility, and cost. Leadership may be hesitant to invest in server security, but by knowing that something will go wrong, it's just a matter of when, you can choose to be on the offense instead of on the defense.

A good tenet of server room security: the more you control, the more secure your servers will be.

Related reading

- BMC Mainframe Blog
- BMC IT Operations Blog
- N-Modular Redundancy Explained: N, N+1, N+2, 2N, 2N+1, 2N+2, 3N/2
- IT Disaster Recovery Planning Explained
- Worst Data Breaches: 4 Critical Examples
- What's Serverless? Pros, Cons & How Serverless Computing Works