



# DATA CENTER SECURITY

Protecting data centers from any potential  
internal and/or external threats

Presented by  
**Charles L. Baxter**



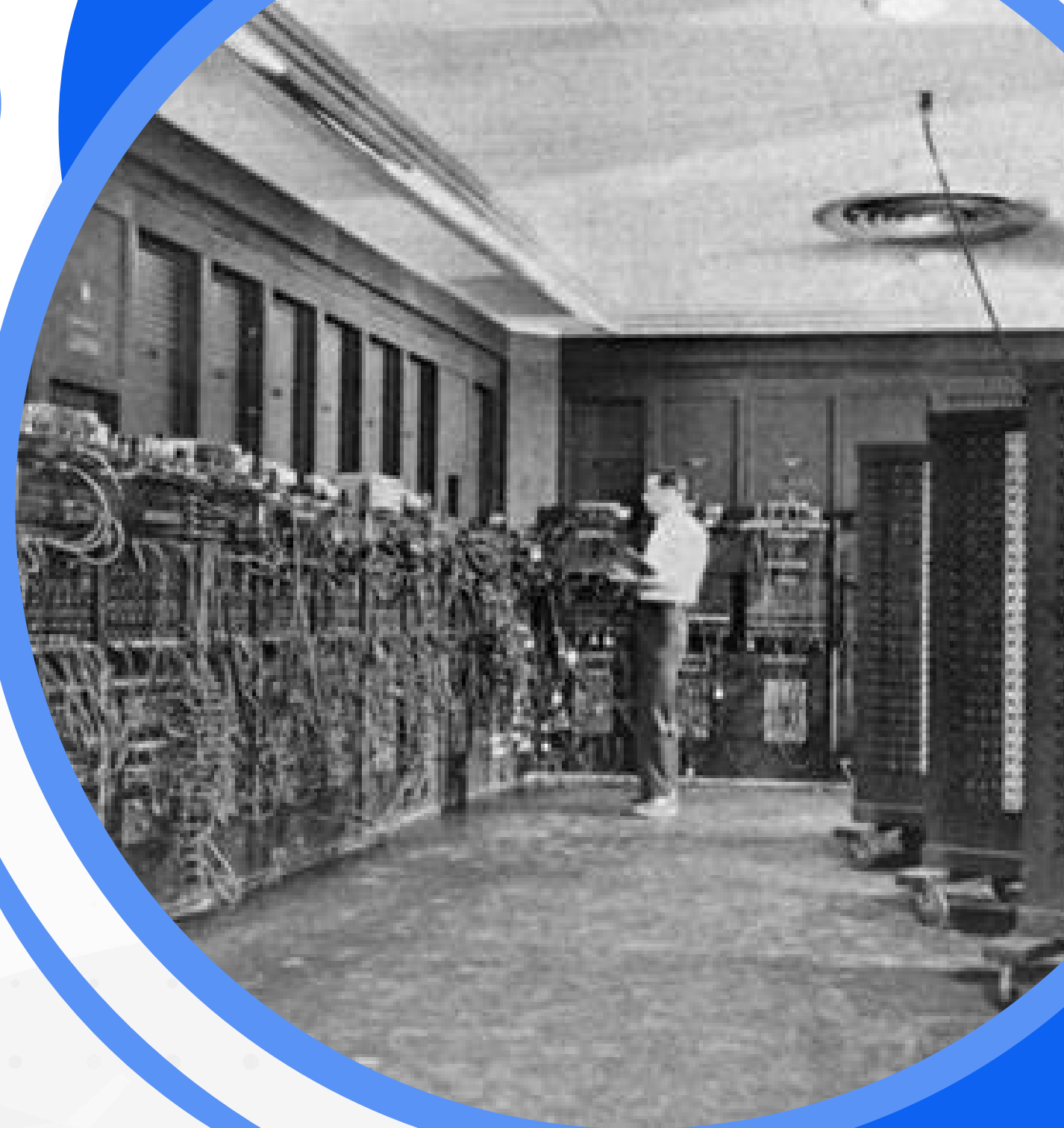
# History of Data Centers

## 1940s

The concept of a data center traces its origins back to the University of Pennsylvania, where the first known data center was established to house the Electronic Numerical Integrator and Computer (ENIAC). ENIAC, often regarded as the world's first general-purpose computer, marked a pivotal moment in computing history. This facility set the foundation for modern data centers by providing a dedicated space to operate and maintain large-scale computing systems.

ENIAC, initially designed during WWII to calculate artillery firing tables, revolutionized military operations with its ability to perform rapid complex calculations. Later, it supported the Manhattan Project, highlighting the transformative potential of computing for both military and scientific advancements.

The ENIAC facility was a simple, secure building with one door and one window. To cool its heat-generating vacuum tubes, it used fans and vents, a rudimentary system that inspired modern data center cooling.







## 1950s

President Harry Truman engaged the CIA to further develop government owned, secret facilities across the country managing data for military and intelligence.

## 1960s

IBM produced a transistorized computer replacing vacuum tubes with transistors while introducing data centers into the commercial space.

## 1970s

Super Computers start to fill data centers augmented by desktop computers.

## 1990s

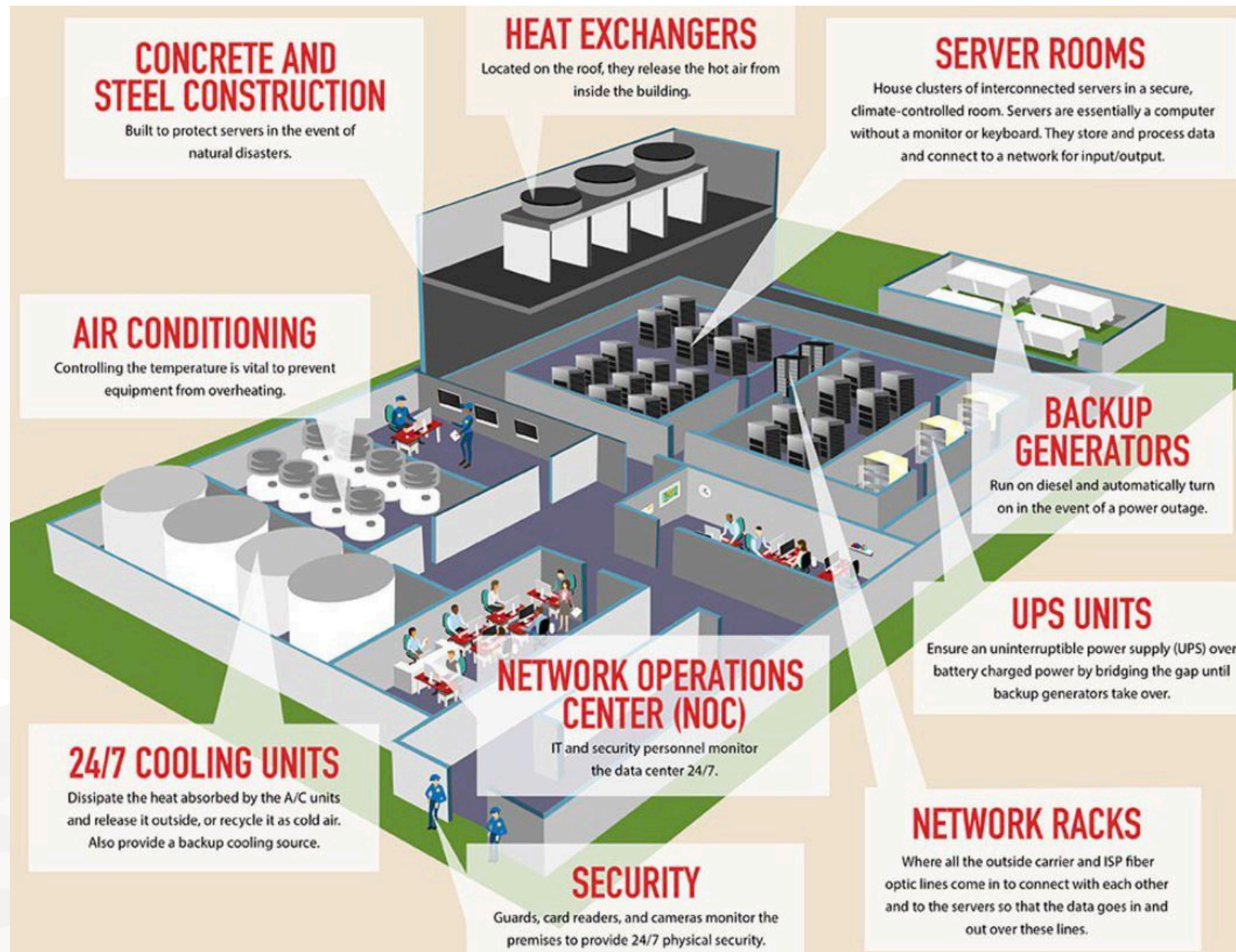
Colocation, or "colo," data centers were introduced to help clients reduce maintenance and software expenses. These facilities offer the advantage of adaptability, enabling businesses to scale and adjust to changing requirements efficiently.

## 2000s

Amazon Web Services (aka: AWS) introduced cloud services.



# Today's Data Centers





# Industry Trends

## Rapid growth

The data center industry is experiencing unprecedented growth, with investments exceeding \$26 billion last year and projections estimating this figure will surpass \$80 billion by 2030. This surge is driven by increasing demand for cloud services, AI advancements, and the rapid digitalization of businesses across industries.

## Cloud Computing

Cloud computing has revolutionized data centers by enabling scalable, on-demand access to computing resources with spending expected to double by 2027.

## Artificial Intelligence

Artificial Intelligence (AI) has transformed data centers by optimizing resource management, enhancing predictive maintenance, and enabling faster processing of complex data workloads, driving greater efficiency and innovation.

## Digital World

The overall digitalization of society has significantly increased the demand for data centers, as they serve as the backbone for storing, processing, and transmitting the vast amounts of data generated by modern digital services and technologies.





# Role of Physical Security

**Recognizing potential threats** is a critical aspect of physical security in data centers. By proactively assessing risks, implementing robust access controls, and monitoring for unusual activity, data centers can ensure the safety of their infrastructure and protect sensitive information from breaches or disruptions.

- ✓ **Physical intrusion by unauthorized parties**
- ✓ **Physical damage to servers, cabling, etc.**
- ✓ **Power disruptions**
- ✓ **Accidental disruptions during installation/maintenance**
- ✓ **Ongoing construction in an active facility**
- ✓ **Remote physical attacks**
- ✓ **Unauthorized movement in the data center**
- ✓ **External hacking of software-based security systems**





**Designing data centers for physical security** involves layered defenses, including secure site selection, controlled access points, perimeter protection, and advanced monitoring systems. These measures safeguard critical infrastructure and ensure operational integrity against physical threats.

- ✓ **Utilizing the appropriate resources:**
  - Design-Build Contractor
  - Security Consultant
  - Data Center Security SME
- ✓ **Corporate Security Standards**
  - Post orders
- ✓ **Design incorporating demographics/client specifications**
- ✓ **Collaboration**
- ✓ **Construction vs. conversion:**
  - Phased approach
- ✓ **Execution**
- ✓ **Personnel:**
  - Monitoring, screening, patrol





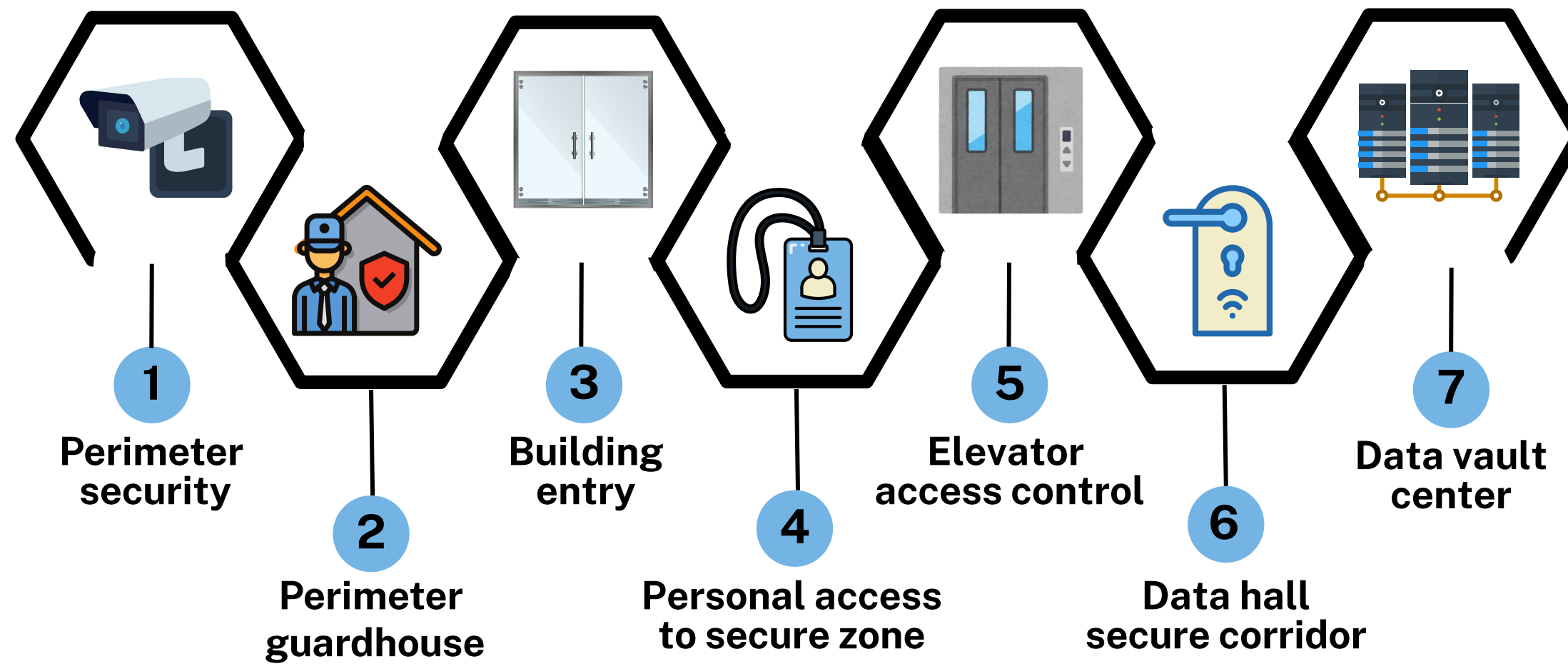
**Effective management and testing** in security measures are essential during planning, construction, and afterwards of data centers. This involves implementing comprehensive security protocols, conducting routine audits, and ensuring compliance with industry standards. Regular testing, such as penetration tests and vulnerability assessments, helps identify and address potential weaknesses before they can be exploited. By combining proactive management with continuous testing, data centers can adapt to evolving threats and maintain robust protection for critical infrastructure and sensitive data.

- ✓ **Management**
- ✓ **Assessment/Penetration testing**
- ✓ **Audits**
- ✓ **Disaster Recovery/Business Continuity Plan**





# Security Technology

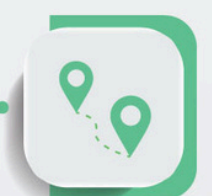




A comprehensive check  
in process that requires  
government-issued identification  
Special badges for visitors



Fingerprint identification



A physical key that can  
provide access to areas  
where equipment is run  
or stored



Badge key cards, which  
can be verified before  
going through doors  
between sensitive areas



Retina or facial scans

## Perimeter protection

Fences, gates, doors, windows, lighting, landscape, bollards, barriers, motion detection, etc.

## Access control (multi-factor)

### Visitor management

- Pre-registration/screening
- Escorts and badges
- Access restrictions

### Intrusion detection

- Monitoring and response
- Real-time alerts



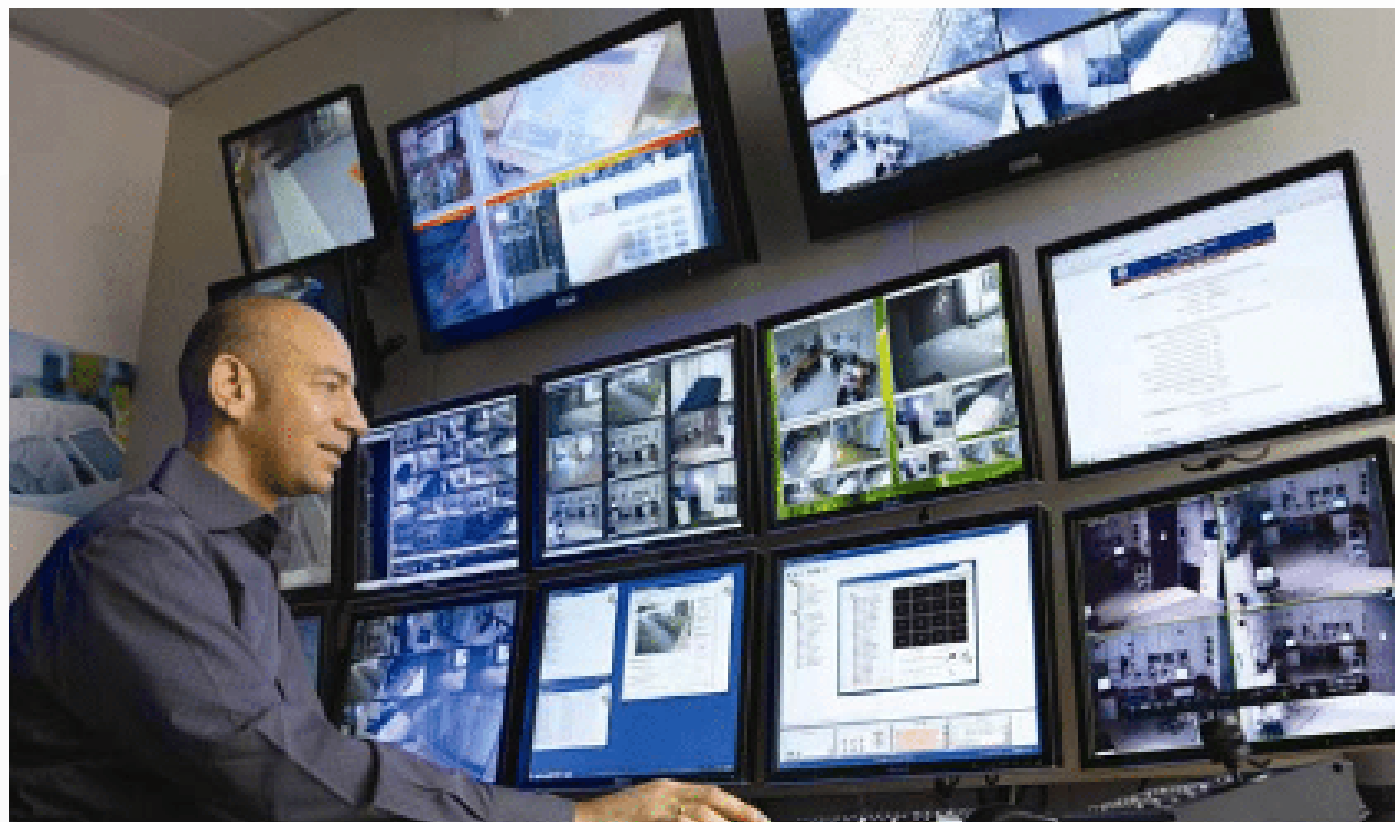


## Cameras

- Deployment and type
- Reactive versus proactive
- Incorporating AI
- Visual tracking
- Quick search
- Enterprise (linked to secure doors, intercoms, mantraps)
- Behavior analysis through AI and other early threat detection
- Drones

## Anti-pass back

## Evidence collection – forensics



# Disaster Recovery & Business Continuity Planning

**\$23,000.00 PER HOUR**  
**Estimated cost of data center outage**

## Business Continuity

Business continuity during a disaster ensures critical operations persist and recovery is swift. It involves proactive risk planning, backup systems, and clear communication to minimize downtime and protect assets, fostering resilience and stakeholder trust.

Effective business continuity planning is vital for resilience and long-term success in the face of unexpected challenges.

## Disaster Recovery

Disaster recovery for data centers focuses on ensuring rapid restoration of systems, data, and operations after disruptions. It involves implementing robust backup solutions, redundancy measures, and recovery protocols to minimize downtime and data loss. Regular testing and updates of the disaster recovery plan are essential to address evolving risks and maintain business continuity.





**Our Disaster Recovery Plan  
Goes Something Like This...**



1. Disaster declaration and notification protocols
2. Site responsibilities
3. Security system recovery
4. Operating system recovery
5. Testing

- Practical
- Tabletop
- Engage local resources

**6. Assembling a disaster kit**

- Back-up strategies
- Facility specific information
- Facility operation guides
- System and application manuals
- Company site contact lists
- Disaster operational guide

# How to Prepare for a Career in Data Security Management

## Education & certifications

- ✓ **CISSP** - Certified Information Systems Security Professional
- ✓ **CISM** - Certified Information Security Manager
- ✓ **CISA** - Certified Information Systems Auditor
- ✓ **CDCP** - Certified Data Center Professional
- ✓ **CPP** - Certified Protection Professional
- ✓ **PSP** - Physical Security Professional





**Technology**



**Professional  
Organizations/Networking**



**Continuing Education/  
Conferences & Workshops**



**Practical Experience**



**Specialized Training**



**Current on Industry Trends**





# Thank You

This presentation is offered as one reference intended to be used as a high-level guide in helping you develop a data center security plan. Physical security design and program management involves a multitude of components working together to achieve the desired outcome which can vary greatly consistent with the type of facility, the client being serviced and any potential internal and external threats.