Uptime Institute®
INTELLIGENCE

RISK &
RESILIENCY

UI Intelligence report 33

Physical security: Technologies and strategies to reduce risk

Authors
Kevin Heslin, Chief Editor, Uptime Institute
Andy Lawrence, Executive Director of Research, Uptime Institute

IT security is one of the big issues of the information age. Billions of dollars are spent protecting the integrity and availability of data against the actions of malign agents. But while cybersecurity is a high-profile issue, all information lives in a physical data center somewhere, and much of it needs the highest order of protection. Data center owners/operators employ a wide range of tactics to maintain a perimeter against intruders and to regulate the activities of clients and visitors inside the data center. This report assesses operator security spending, concerns, management and best practices.

30-45 minutes to read

UII-33 v1.1 published November 20, 2019 last updated December 2, 2019

This Uptime Institute Intelligence report covers:

ABOUT UPTIME INSTITUTE INTELLIGENCE

Uptime Institute Intelligence is an independent unit of Uptime Institute dedicated to identifying, analyzing and explaining the trends, technologies, operational practices and changing business models of the mission-critical infrastructure industry. For more about Uptime Institute Intelligence, visit https://uptimeinstitute.com/ui-intelligence.

KEY FINDINGS

- **Spending on physical security is commonly around 5% of the operations budget but in extreme cases can be as high as 30%.**
- **Data centers employ a range of common technologies and techniques to control access to the facility, but there is no “one size fits all” solution to physical security: each organization must tailor their approach to fit their circumstances.**
- **Neither cloud-based data replication nor the threat of cybersecurity to both IT systems and facilities equipment have significantly diminished the need for physical security.**
- **Most data center owners and operators consider unauthorized activity in the data center to be the greatest physical threat to IT.**
- **Access to the data center property is governed by policies that reflect the business requirements of the organization and establish the techniques and technologies used to ensure the physical security of the facility. These policies should be reviewed regularly and benchmarked against those of similar organizations.**
- **Data centers commonly employ third-party security services to enforce physical security policies.**
- **Attempts at unwarranted entry do occur. In a recent study, about one in five data centers experienced some form of attempted access in a 5-year period.**
- **Drones, infrared cameras, thermal scanners and video analytics are promising new technologies.**
- **Biometric recognition is still viewed skeptically by many operators.**

Introduction

All IT-based information and services reside in a data center somewhere; unauthorized physical access and improper actions by authorized staff represent a critical risk to data integrity and service availability and therefore demand constant vigilance.

Physical breaches are among the chief information officer’s biggest worries. Unauthorized access to information and destruction and loss of integrity to data and services are major concerns. So, too, is any loss of key services due to on-site technology or process failures.

Uptime Institute Network’s data shows that in the 5 years between 2012 and 2017, about one in five data centers experienced an attempt at site access and about one in 10, an attempted perimeter breach. This data aligns with a recent informal Inside Track (online) poll, in which 25% of respondents reported some sort of unwanted activity and with in-depth interviews with seven data center owners/operators globally, who reported mostly policy violations.

Owners/operators view this unwelcome activity as a general risk to the data center, to IT services, and to personnel. However, stringent security cannot simply eliminate all access to the data center. Customers, vendors, facility staff and other personnel need to access even the most sensitive white spaces to perform maintenance, repair and replace equipment; change equipment configurations; perform assessments; or accommodate growth or consolidation. In some facilities, executives and sales staff may also have a business need to access to the data center.

Many security incidents are not truly threats to the data center, although they have the potential to become so; rather, they may be accidental breaches of guidelines or policy or a casual disregard of rules. In one unusual case, a data center operator reported that some local residents would access the site as a shortcut — in some cases, even scaling a fence, until its height was increased.

A particular challenge, according to data center owners and operators, can be characterized as “the trusted threat,” where vendors, staff or visitors misbehave, either maliciously or inadvertently. In these instances, background checks, variable access and security escorts usually prove effective.

In addition, data centers can be dangerous places, and security can help reduce the likelihood of injury or even death by limiting access to generators, switchgear and other equipment to qualified vendors and staff.

To better understand the security concerns of data center operators, Uptime Institute reviewed security-related data from Uptime Institute Network’s 2017 security benchmark survey; reviewed issues that have been raised at roundtables, industry events and in Inside Track discussions; and interviewed seven data center operators in October and November 2019 (six of whom are Uptime Institute Network members) about their security practices and experiences. Notes from these interviews are provided in the **Appendix**.

Physical deterrents

All data center owners and operators that Uptime Institute engages with have embraced physical security as a requirement for their facilities and operations. In some extreme cases, the security measures include moats, razor wire-topped fences and armed security guards. At government and military installations, or even in cases where the business risk from an incursion is extremely high, such extreme measures may be warranted. In other cases, however, data suggest security risks are quite low.

Because of the wide risk range, and the varying costs in differing geographies, the cost of physical security may vary widely. In interviews, most operators told Uptime Institute they spend between 5-8% of their operational budget on physical security. However, there are outliers: one operator spends 30% of its annual operations budget on security, while another spends 20%.

The level of security required by a data center depends in large part on the business activities and processes conducted on the systems in the data centers, as well as factors such as location and who knows of its existence.

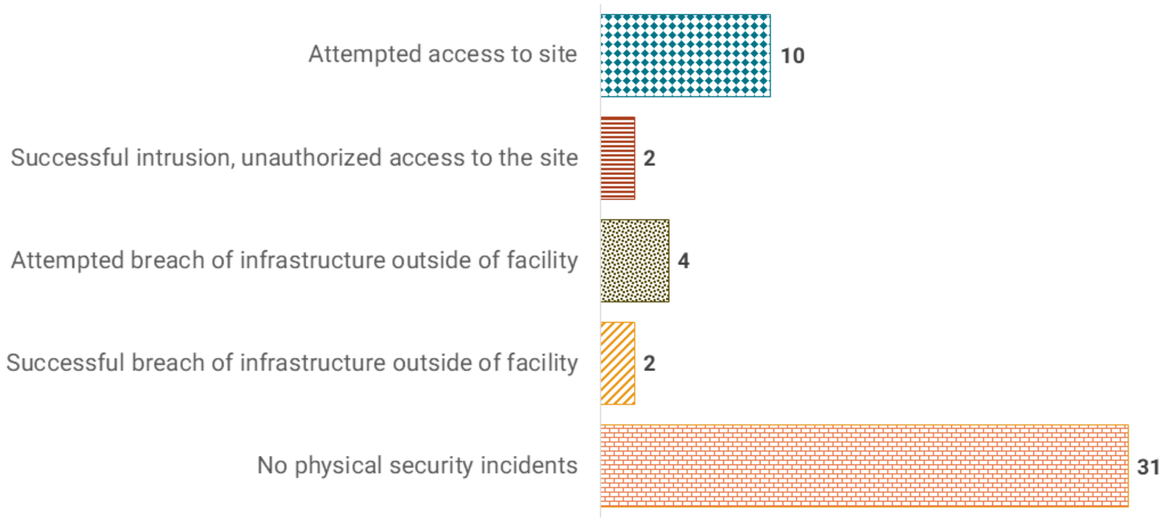
Some data center owners and operators maintain relationships with security specialists. These firms help them develop appropriate security plans that consider the organization's business requirements and any site-specific threats. Their plans are subject to periodic review to address new considerations that may evolve over the life of the data center (e.g., increasing crime rate in the area) or any sudden developments that increase the security requirements, such as nearby roadwork or construction.

Periodic and regular reviews do not fully satisfy all organizations. Uptime Institute identified several firms that had contracted with security penetration vendors, tasked with evading the various checks set up in an organization. In some cases, these firms were hired not by IT management but by another department, effectively increasing the challenge of detecting them.

How real is the risk?

Calculating the risk of a physical intrusion, or assessing how much should be spent on security, is not straightforward. Some organizations are targets because of what they do, while others may be in politically unstable parts of the world (in one case, an Uptime Institute client's data center was visited by armed forces during a security crackdown).

In 2017 Uptime Institute surveyed about 50 Network members, asking how many had experienced a physical security incident in the past 5 years. The members reported 10 instances of attempted access to the site and two successful intrusions. Additionally, there were four attempted breaches of the infrastructure outside the facility and two successful breaches (see Figure 1). Most users believe these attempts more than justify their efforts to prevent unauthorized access to the facilities.



Has your organization experienced a physical security incident in the past 5 years? (Select any that apply)

Source: Uptime Institute Network Benchmarking Survey 2017, n=48

UptimeInstitute | INTELLIGENCE

Figure 1. **Companies experience few serious threats from outside.**

This data is limited, but if it is representative — that is, if about a third of data centers have experienced some sort of physical security incident — can this be translated into real damage in terms of financial or reputational losses or some other problems, such as compliance breaches? Unfortunately, at present, neither Uptime Institute nor any other research that we are aware of is able to answer this question. However, we can draw some provisional conclusions from the absence of data.

First, in the nearly 20 years that Uptime Institute has been collecting AIRs (abnormal incident reports) data, we have not recorded a single incident of a data center outage being caused by malicious action (although we have recorded many incidents of human error, which could have been caused by unauthorized actions). Second, unwanted data center intrusions have not become a major, headline-grabbing issue in the way virtual intrusions (i.e., malicious hacking and fraud) have.

Financially motivated crime has never been a big problem for the physical data center (although in the 1980s, the very cost of memory chips and poor physical security did lead to some thefts at smaller data centers). In rare instances, thieves might steal unprotected or lightly protected physical servers to obtain valuable data as part of blackmail, ransomware or corporate espionage plots. In one highly publicized incident, approximately 600 bitcoin servers were stolen in Iceland. While the servers and associated equipment had significant value, the perpetrators wanted to deploy them as an illicit bitcoin mine.

But this is not to encourage complacency: awareness of data centers and their critical role is becoming much more widely known and understood. Terrorist groups, hostile states, and even environmental campaigners could conceivably act against data centers — indeed, there have been examples where data operations have been disrupted by remote access. Given the potential impact of a serious physical incursion, the current level of vigilance and the expense will be regarded as justified by most management teams.

Data security

How is cloud and Internet technology changing the need for physical security? There are two main impacts:

- First, the ability to more easily and near synchronously replicate data at secondary locations has, to some extent and at least in theory, reduced the level of dependence on physical equipment and IT gear in data centers.
- Second, the threat to facility equipment, now commonly possible via Internet connections and remote management, has introduced a new set of threats for facility management teams.

Cloud resiliency

The use of multi-site, cloud-based resiliency has opened up many new possibilities for enterprises. Many are eliminating secondary back up data centers, moving to disaster recovery as a (cloud-based) service; others are moving some of their workloads and data to the public cloud.

In theory, protecting single sites and equipment may be less critical than it once was, at least for some clients. However, Uptime Institute research shows that distributed or cloud-based resiliency does not necessarily eliminate the risks or consequences of single-site failure, so most operators, including public cloud operators, still invest heavily in site-based resiliency — and, of course, on site security. Public cloud providers, because of their high profile, not only have high security themselves, but insist their colocation partners also meet high standards.

Cloud-based replication does make it easier and cheaper to store data and run applications elsewhere. While this does not make it less important that each data center is adequately protected, it does provide a level of insurance in the event of a serious incursion.

Equipment vulnerability

According to one online poll of Uptime Institute Network members, many data center managers are becoming more involved with information security. This is not surprising: there is a growing concern that physical equipment such as power distribution units, generators, uninterruptible power supplies (UPSs) and transfer switches are now becoming vulnerable to hacking.

In 2017, for example, researchers at the Idaho National Engineering Laboratory demonstrated that it is possible to remotely hack into a control system for an electrical generator. Their demonstration included a dramatic explosion. Efforts such as these are made easier when vendors inadvertently create new vulnerabilities, making it increasingly important that cyber and physical security efforts are coordinated.

In their book “The Fifth Domain,” Richard A. Clarke and Robert H. Knake report that successful cyberterrorism efforts often exploit weaknesses in vendor IT systems, including those involved in construction and maintenance. Clarke served as White House counterterrorism coordinator under Presidents Clinton and George W. Bush. Knake served as President Obama’s director for cybersecurity policy at the National Security Council.

Unauthorized access

The list of security concerns for an operator is extensive and requires careful thought. Setting aside the least likely threats (terrorist attack, etc.) and the somewhat separate issue of virtual/cyber threats, most managers/operators focus on reducing or eliminating unauthorized access.

Data center operators are concerned about four categories of unauthorized physical access. These include:

- Unauthorized site access.
- Unauthorized facility access.
- Unauthorized access to white spaces and racks.
- Unauthorized access to customer spaces, in the case of colocation providers.

Data center facilities have vulnerabilities at each of these levels. It is not necessary for an individual to gain building access, for example, to do significant damage to data center operations — they could sabotage equipment, such as generators, located outdoors.

Similarly, trusted individuals inside the facility can impact operations in variety of ways. In extreme examples, they could depower servers and other equipment, damage network equipment, cut fiber paths or steal data from servers or wipe them, among other concerns. In the past, there have been cases of individuals, and court cases, resulting from damage done in this way. Unfortunately, data centers cannot simply screen for trusted individuals with bad intent.

For obvious reasons, organizations never allow unqualified individuals access to sensitive IT gear. This doesn’t prevent problems; according to Uptime Institute research, more than 60% of data center outages are caused by human error, such as activating an emergency power off (EPO) system or performing maintenance on the wrong equipment.

These incidents can be sometimes limited by security policies and monitoring that restrict the movement of staff and vendors to pre-approved areas listed on work orders or similar documentation.

The following sections suggest just some of the many problems that data center owners/operators must guard against, at various levels of access.

Threat 1: Site access

Owners and operators begin the screening process as far from the data center white space as possible, even extending to monitoring and protecting remote equipment and utility services. This includes connectivity outside the perimeter, if possible, to ensure reliable power, water, and communications services. Loss of these services can be catastrophic to data center operations. Redundancy and pathway independence are essential.

Threats to operations increase inside the site perimeter. Major gear such as generators, cooling towers and even utility substations are often located in relatively open areas on the site. In addition, even dedicated data centers must manage a flow of legitimate traffic, including deliveries, visitors, maintenance and management personnel, IT, vendors and inspectors. Colo facilities must also expect customer visits.

The threats multiply in mixed-use facilities. In these facilities, critical and non-critical functions may share critical building systems, such as generators, cooling towers and even utility service entrances. As a result, access to this sensitive equipment may not be limited to qualified mission critical staff. If this is the case, a detailed, multi-party study is required to restrict and manage access (remote, micro data centers may also present particular challenges).

Physical security should be considered at an early stage of data center development; local site conditions can dictate some of the tactics and technologies deployed to provide physical security — and the ongoing costs.

Data center managers interviewed by Uptime Institute detailed a rather lengthy list of criteria to considered before a site would be approved for development. Environmental conditions, including storm frequency and flooding, topped the list, closely followed by physical safety and political climate.

Threat 2: Facility access

Inside the perimeter, access to the data center is generally through a secure lobby, with occasional exceptions for deliveries through a loading dock. Accessing the lobby generally does not increase risk to IT; however, the lobby is rarely the endpoint of a data center visit. Legitimate visitors will generally require admittance to more sensitive areas. Precautions are required to secure the safety of these visitors as well as equipment such as generators, chillers, UPS rooms, batteries and transfer switches.

Threat 3: White space and rack access

Racks and white spaces are the most vulnerable areas in a data center. Having access to servers generally provides unparalleled opportunities to damage IT operations, either intentionally or inadvertently.

Although few visitors are generally allowed access to server areas, any access multiplies the chance of human error. Vendors and staff can access the wrong equipment, defeat dual-server configurations, misplace perforated floor tile or fail to restore breaker settings after maintenance. Training exercises have, in the past, led to some major outages, with both trainees and trainers making mistakes.

In some instances, workers violate policies and procedures regarding food and beverages, and in others, they might affect airflow by leaving doors open or using underfloor areas for storage/refrigeration. Other risks include inadvertent activation of fire suppression systems or even fire.

In addition, access to these areas allows opportunities for intentional bad acts, such as stealing data, damaging hard drives, corrupting data or introducing malicious code.

Colocation companies have a particularly difficult challenge managing white space and rack access. Their customers may sometimes increase risk simply because of their need to enter shared white spaces or have vendors perform maintenance on their behalf.

There are differing views of the benefits of escorting trusted staff and engineers. Many facilities insist all visitors and third parties, however well qualified and trusted, are escorted to ensure facility policies are followed. In other cases, facilities will provide temporary access to vendors who have completed training. Sometimes these facilities will first escort vendors to their work site before leaving them to work unsupervised.

The practice of escorting vendors:

- Improves security.
- Reduces policy violations.
- Increases staff or security guard requirements (cost).

Many operations feel that allowing access to properly vetted and trained vendors does not pose a major security risk and that increased cost of escorting them does not provide significant benefits.

Threat 4: Colocation

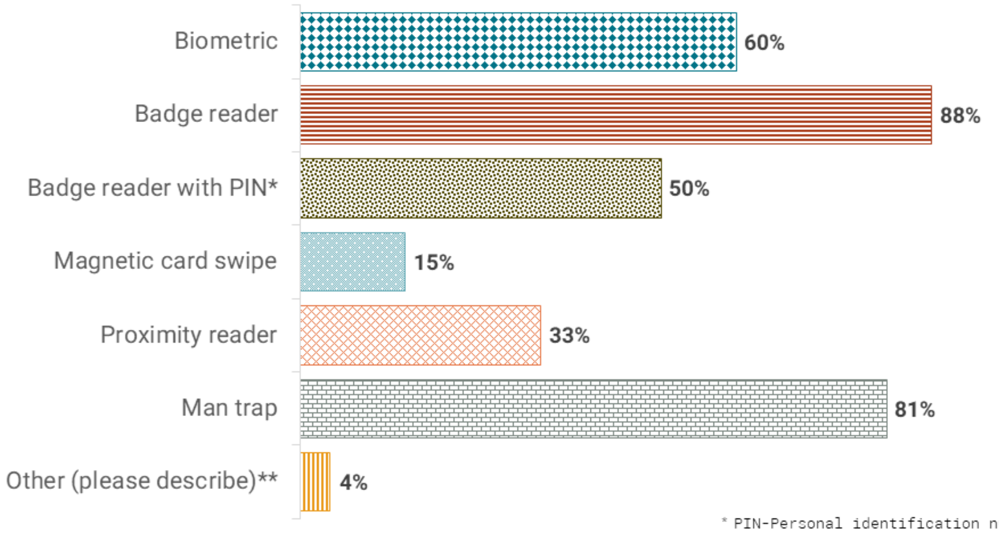
Customers in colocation facilities will usually be responsible for securing their own suites, cages and racks, usually using electronic or mechanical technology (locks, biometrics, card readers, etc.), and they must authorize any entry to their cages. They are responsible for screening vendors and other visitors, but they must also abide by all facility policies, including use of security escorts when applicable. Colo customers may deploy cameras, but facilities will limit their field of view to the customer's rack, making remotely controllable pan-tilt-zoom (PTZ) cameras problematic in some facilities.

Security technologies and techniques

Data center owner/operators combat access risks using a variety of security technologies, such as biometric readers, man traps and security badges. These technologies will be familiar to all data center professionals; although some form of technology-based security is nearly ubiquitous, the actual technologies vary widely.

Common technologies have high adoption rates

The Uptime Institute Network 2017 security benchmarking survey found high adoption rates for a broad range of technologies used to regulate admission to facility and rack space areas (see Figure 2). Further research is likely to show that because of site configuration, cost, space and management overhead, different classes and sizes of data center are likely to favor particular technologies.



* PIN-Personal identification number
** Metal detectors, bag X-ray; anti-piggyback detection

What type of physical security is used at the data center? (Select all that apply)

Source: Uptime Institute Network Benchmarking Survey 2017, n=48

Uptime Institute | INTELLIGENCE

Figure 2. **Many security technologies have a high level of adoption.**

Other common security technologies used in the data center include locked racks, cages, cameras, bullet-resistant glass and alarmed doors. All respondents to our 2017 security survey reported the use of cameras.

Data center operators use a variety of physical barriers to protect their perimeters and sites. Depending on the site, these may include high-security fences, razor wire, concrete walls, gates, bollards, water features (moats), vehicle traps, berms and landscaping. Cameras, including PTZ and infrared versions, provide further security. Even the building infrastructure — thick concrete walls are common— can be part of the security scheme. As a complement to these active security measures, most data center owners and operators hide their buildings "in plain sight," limiting or even eliminating any signage that might indicate ownership or function, even on trucks or uniforms.

Biometrics in the data center

Data center owners and operators express a great deal of skepticism about the use of biometrics as part of physical security programs, according to interviews and Uptime Institute Network member feedback — although the promise of biometrics (fingerprint, voice, iris and facial recognition) means it is constantly being tried.

IT executives familiar with biometric technologies noted that they are not stand-alone security systems. Biometrics must be combined with a variety of more familiar technologies such as man traps, proximity readers and access control systems to be effective. A financial services chief information security officer put the issue succinctly, "A better question might be when is (facial recognition) a good fit. It can be very expensive and finicky, but in certain circumstances a good alternative. However, nothing takes the place of well-trained staff and best practices such as man traps and video surveillance."

Early adopters expressed frustration at the number of false readings and alarms raised by biometric systems, especially when using less expensive equipment. More expensive equipment tends to be more effective but can be cost prohibitive.

Advanced biometrics can also pose unexpected security risks and inconvenience — especially in the aftermath of a breach. "Claims by biometrics vendors that their credential stores are secure and can't be hacked should be treated with great caution," said one skeptic.

Guards

While they may be high profile — and effective to a point — security does not rely primarily on guards and technologies. These are only tools for enforcing policies that reduce unauthorized access to the wider data center site and white spaces and other sensitive infrastructure facility. They also help to manage personnel within the facility, limiting staff, vendors and visitors to authorized activities and areas.

Almost all data centers (94% of 2017 Uptime Institute Network survey respondents) employ 24/7 security guards to screen and monitor visitors, monitor cameras, patrol grounds and respond to alerts from cameras and other devices; some may also be trained to report IT alarms in some facilities. Security guards are often among the lowest-paid employees, potentially introducing certain risks. However, they often must pass background checks and complete training before gaining access to sensitive facilities spaces.

As security guards are often directly employed by third-party providers, these firms generally conduct background checks, often with oversight or approval from the data center owner/operator. The data center conducts training of site-specific duties and policies and issues credentials. Security guards at some data centers are armed.

There are limits to what even a dedicated security team can accomplish. As a result, guards at most facilities are unarmed (especially outside the United States) and may have other duties, such as reception, responding to alarms and activating call-down procedures, when warranted. Their presence, and the intimidating façade they project, along with the high walls and gates, high-tech cameras and devices, will discourage all but the most ill-intentioned and well-armed intruders. If there is a potential for conflict, security guards are generally trained to call local law enforcement.

At the same time, well-trained security guards following well-thought-out and communicated policies can prevent a lot of unintentional and inadvertent problems by limiting access to authorized personnel with legitimate reasons for entering the data center or other areas of the facility. Guards familiar with the data center can escort vendors to the right rooms or even to a particular rack. Such security can also reduce the likelihood that an unqualified individual will touch an EPO or that a technician will breach procedures, such as eating/drinking in a white space.

Security may also enact policies to prevent the risk that memory devices such as universal serial bus (USB) drives pose to the data center, with guards and inspections required to make these policies effective. This issue concerns many IT organizations; some use their IT service management system to universally disable USB ports, unless the technician is authorized with an access code.

In some cases, extreme security measures may also serve a marketing purpose. Just as owners and operators have embraced the need for physical security measures, so have customers. Potential clients want to believe that their assets are protected, and the visible on-site security help to reassure them; some colocation clients include exacting security provisions in their request for proposal documents.

Policies

All the security measures taken by data center owners and operators amount to little without a coherent set of policies. These policies reflect the business requirements of the organization, which will dictate access levels as well as the use of technology and security guards. These policies, or subsets of the policies, should be available to all the appropriate staff and visitors and should be regularly reviewed and benchmarked against similar organizations. Many organizations also post these policies prominently.

Some organizations develop their risk profiles and policies in tandem with an external security provider. These profiles are updated regularly or whenever there is a change in the environment, such as nearby construction, local crime or even a new high-profile client.

Factors to consider in a review include the risk profile of the organization as well as business requirements, such as data center purpose, external audits, regulatory requirements, customer satisfaction and cost.

Ideally, the organization will evaluate these factors early in the design process, as the first line of access control features — including exterior walls, site features, access features and security control rooms — should be incorporated in the facility and site plan.

Although not a policy guide, the **Questions to ask about data center security** checklist includes areas to consider when developing policy guidelines and during reviews.

The data center operator will also need to consider and develop a system or set of rules that provides suitable access to everyone with a legitimate reason to pass through perimeter security and/or enter the data center. Interviews conducted for this report by Uptime Institute suggest that data center owners and operators generally offer some level of access to:

- **Staff, especially senior data center management -** Having building-wide operations responsibility makes it imperative that these individuals can access all areas of the facility. Technicians will, of course, be authorized to enter only designated areas to perform required duties.
- **Security guards -** Performing duties such as escorting vendors, walking rounds and responding to alerts requires access to all but the most sensitive white space and dangerous equipment areas.
- **Vendors -** Third parties and vendors charged with maintaining IT equipment and building systems must have access to these systems — but not to other areas. Some facilities require these individuals to be escorted at all times.
- **Visitors, including non-mission critical staff -** The level of access for visitors and non-mission critical staff will vary according to the purpose of their visits. Customers will have access to more spaces than meeting attendees. Code enforcement officials will require even greater access. These visitors will be escorted at all times in almost every facility.

Conditions will be different in colocation facilities, where security and even senior staff may be denied entry to data halls unless they have the permission of the customer. Similarly, the colocation operator and customer must coordinate to ensure that the customer and its visitors and vendors clear building security to gain access to the customer's spaces.

Questions to ask about data center security

Facility staffing

- Is the facility staffed 24/7?
- Do you use a third-party security specialist?
  - Does it conduct background checks?
- How many individuals are on each shift?
- Are security guards armed?
- How do they respond to intrusions such as trespassing?

Perimeter access

- Is the perimeter controlled by security (crash-resistant) fencing?
- Is the main gate staffed or remotely controlled?
- Is there a vehicle trap?
- Are vehicle barrier controls in place?
- Are external mechanical yard components situated within a fenced area with barriers?
- Are grounds monitored by security patrols, infrared/thermal cameras or other sensors?
- Do signs or truck markers identify the purpose of the facility?

Facility access

- Is the loading dock secure?
- Are access control systems, such as badge readers, proximity readers, man traps, cameras, biometric (e.g., fingerprint monitoring) systems in use?
- What is the process to manage access credentials?

Policies

- Does the facility accept unscheduled deliveries?
- Can the facility be accessed 24/7 by accredited visitors (including contracted vendors)?
- Are vendors escorted when working in the facility?
- How are vendors vetted?
- Are vendors issued work orders, including start and stop times?
- Are staff, vendor, and other credentials reviewed? Audited?
  - How often?
- Are security plans reviewed/updated?
  - How often?

Common threads

In addition to the survey, Uptime Institute interviewed operators regarding their policies and use of technologies. Each interview addressed the following topics:

Systems and access

Our interview participants all described detailed systems and policies dedicated to limiting access to authorized personnel, with different levels of access for different personnel. The organizations all used automated systems to authorize access to the data center and issue credentials, with most working in conjunction with a work ticket system and the human resources (HR) department to validate identities, employment status and the reason and timeframe of the authorization.

In one fairly typical instance, tags and badges are issued to everyone who needs access to the data center, with the data center manager reviewing every request. The data center security manager or IT manager determines the access level and logs the authorization into an access system. Staff credentials are revoked or updated automatically whenever HR logs a change of employment status. One facility issues credentials on a 90-day "use it or lose it" basis, with the access database audited on an annual basis. In this instance, the data center is also subject to Sarbanes-Oxley audit requirements. At all interviewee sites, visitors are issued daily badges in exchange for identification and are escorted at all times.

Background checks

Most of the organizations interviewed for this report require security guards and data center staff to pass annual background checks, with one organization mandating annual drug tests and training for security guards. The security guards and data center staff at one facility are issued permanent credentials, which must be returned at the end of each shift.

Managing vendors

According to the interviews, all the organizations required vendors to present and exchange government-issued identification (ID) and work tickets, including detailed specifics about the work to be performed, in return for daily badges. Most organizations streamline this process for "trusted" vendors by adding them to a pre-approved access list. These vendors must provide current proof of in-house training as well as the government ID and work ticket.

Vendors are escorted in most (but not all), facilities, with at least two allowing vendors to work unsupervised after being escorted to the proper location. Vendors must submit to a variety of additional requirements. They are only admitted to one facility, for example, when staff engineers are also on site, as service vendors are not allowed to switch or manipulate equipment.

Memory devices/plug-ins

In about half the facilities. computers and portable memory devices are allowed even in rack areas but only if required for a work assignment, as presented in the facility's training program. At one facility, media storage devices are destroyed when the work is complete, and another requires laptops to remain on assigned worktables.

Security packages

In many facilities, security does not sign for or accept any deliveries, but there are exceptions. One facility has dedicated unionized shipping and receiving staff, who scan and process packages and will accept unscheduled deliveries depending on what is being delivered and staff and forklift availability.

Policing role

It is also almost universal practice that security guards and staff will also monitor the facility and will note and report policy violations. Severe or repeated infractions can lead to termination of employment or facility bans.

Conclusions and recommendations

Physical security remains paramount in the data center industry; most organizations see it as an essential complement to online (cyber) security. Although physical security measures may appear unglamorous and are often low tech, breaches can have very serious consequences.

New trends in data security and the emergence of cloud-based services and replication will not reduce the need for physical security, because without good physical security, the entire virtual edifice is vulnerable.

The level of data center security should be determined by business requirements, with frequent re-assessments. In some cases, data center owners and operators may find a simple system of pre-authorization and access control to be sufficient.

Most data centers employ multiple technologies with the goal of limiting access to sensitive areas to those with a business requirement. Care must be exercised when deploying these technologies so they do not impede legitimate access. In addition, to be effective, the technologies must be deployed in tandem with a credentialing system to support policies developed by the organization.

An overall security policy document is important. The policies and access lists must be regularly updated and shared with stakeholders.

Appendix: Interview Notes

Interview 1

SNAPSHOT	
Company revenues	Not available
Individual interviewed	Datacenter Facilities/Operations
Industry	Colocation
Budget dedicated to security	30%
Region	Asia-Pacific
Facility type	Colocation

This colocation company is just in the process of ramping up, but it already maintains a full array of physical security features and outsourced 24/7 security. The facility boasts eight levels of security from the data center's main entrance to the data hall. The operator reports no incidents to date.

Perimeter

The data center perimeter is protected by ASTM International K4-rated anti-climb perimeter fencing (3 meters high). Vehicles must pass through a staffed security gate and a vehicle trap before gaining access to the site. They are also subject to undercarriage and internal checks.

The concrete construction provides an additional level of security against vehicles, with ASTM K12 anti-crash barriers further protecting the entrance. Security conducts regular patrols of the grounds, which are monitored by a variety of PTZ and fixed infrared closed-circuit television (CCTV) cameras.

Interior

All visitors to the site receive a copy of the physical access procedures. Access from the lobby requires pre-authorization from operations and is limited by a man trap. Individuals and packages must also pass through a metal detector, which is monitored by fixed and PTZ CCTV cameras and patrolled regularly by security. Additional technologies employed include a radio-frequency identification access card reader, proximity reader and freight vestibule.

Policies

Access to the data center is granted only through the electronics visitor management system (EVMS), which requires visitors to log in in advance, provide details regarding the visit — including purpose and duration — and specify the time and date of the visitor. All visits are subject to approval by the operations team.

Interview 1 *(continued)*

All visitors must provide government-issued ID. Vendors, security and staff have greater facility access, depending on job function, but are still subject to EVMS approval. While vendors can obtain pre-approval for extended projects, they (and all visitors) must be escorted at all times by security.

The loading dock is also secured, and unscheduled deliveries are not accepted. Other packages are subject to scanning.

Biggest risk

None mentioned.

Other notes

The data center follows security guidelines described by the Monetary Authority of Singapore (https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines--21-June-2013.pdf).

Security will respond to, report and correct policy violations, which can have severe consequences. More serious incidents, such as armed intruders, will be reported to the police.

Local conditions suggest there is no need for armed intruder training.

The facility does not prohibit the use of outside computers, tablets or removable storage devices. The organization has closed all unused ports and has also completed internal/external network vulnerability assessment and penetration tests on the facility’s internet protocol addresses and infrastructure.

Interview 2

SNAPSHOT	
Company revenues	>$1 billion
Individual interviewed	Manager of data center security
Industry	Transportation
Budget dedicated to security	20%
Region	North America
Facility type	Dedicated

This facility incorporates a broad range of physical security measures, including two-factor access control with the potential to require three-factor control in response to a government mandate. Security personnel are provided by a third-party vendor, with each employee approved by the manager of data center security. The facility has not had a serious incident in the past 5 years.

Perimeter

Physical barriers at the gate include an 8-ft high, cable-reinforced K4-rated fence. Access is through sliding gates, with entry to parking lots controlled by reinforced arms. The building is a concrete-reinforced structure rated to withstand EF4 (Enhanced Fujita Scale 4) winds (i.e., 166-200 miles per hour). The building is unmarked and difficult to recognize.

During business hours (7 a.m. - 3 p.m. weekdays), access to the site is through staffed guard shacks and sliding gates at the entrances. At those times, parking control gates are open. At other times, the reverse holds true. Vehicles are not inspected.

Interior

Interior precautions include fixed and PTZ CCTV cameras, biometric recognition systems, proximity readers and a man trap. Ordinarily the facility employs two-factor authentication, but the facility is subject to a mandate to employ three-factor authentication when requested by a government agency. At these times, a personal identification number (PIN) is employed. Three-factor authentication has little or no effect on data center operations.

Policies

The data center employs a visitor registration system, which it uses to enforce five levels of access, ranging from three levels of limited visitor access to full access for security and IT staff. Vendors receive no higher than Level 3 access and are escorted at all times.

Applications for access to the data center are approved by the facility manager, with the security manager or IT manager finalizing the appropriate access level. The process normally takes 24 hours or less. Access lists are updated continuously, with internal and Ernst & Young audits every 6 months. Penalties for violations vary by infraction.

Interview 2 *(continued)*

Unionized labor will accept unscheduled packages, but these, as well as scheduled packages, remain on the loading dock until accepted by the proper party. Laptops and storage devices on a rolling table are allowed on the data center floor, but only when required for the work assignment.

Biggest risk

Trusted insider.

Other notes

- Security presence is greater during business hours, with assignments rotating on a 2-hour basis to maintain alertness levels.
- All facility personnel receive active shooter training (run, hide, fight).
- Drones are viewed as a possible future security measure.

Interview 3

SNAPSHOT	
Company revenues	$100-$500 million
Individual interviewed	Data center security manager
Industry	IT/Technology
Budget dedicated to security	8%
Region	Europe
Facility type	Dedicated

This facility has an advanced ticketing system that enables the data center security manager to exercise oversight of activities on the site. In addition, the facility deploys an extensive array of technologies to address access and egress to the site. The facility reports only low-impact incidents in the last 5 years.

Perimeter

The perimeter is surrounded by an 8-foot high fence, with perimeter sensors and concrete barriers to protect against vehicles. Guards at the gate check visitors against a register held in the facility's security office. Upon passing through the gate, visitors encounter no further checks or inspections, except a vehicle trap. The building is unmarked, but trucks entering the facility may provide some hints as to the purpose of the building.

The facility is also monitored by military-grade thermal scanners, which enables the data center to monitor outside the perimeter and even helped neighbors who were being burgled.

The facility also deploys CCTV.

Interior

The facility operates a full array of technologies, including biometric (facial reader), badge reader (temporary access), badge reader with PIN (cards do not leave site), proximity reader, man trap and freight vestibule. Before passing through the lobby, visitors first encounter security guards, who are protected by bulletproof glass.

Policies

The overall security scheme includes an IT system and recognizes different kinds of access, with different privileges at each level, depending on work requirements: permanent access for staff and colo customers, temporary access, and outside temporary access. All are subject to house rules. Vendors can move unescorted through the facility after training and passing a house rules test.

The facility reviews these access levels annually.

Final approval of access is approved by the security department, but it is multi-step process that begins with the request, which is then reviewed by the data center manager, then a remote security team and, finally, by a data center security manager.

Interview 3
(continued)

Unexpected packages are not accepted. A security ticket is opened for other packages, then they are tagged, labeled and stored in a locked area.

Biggest risk

The wells containing dark fiber, especially the second set of wells, which are outside the perimeter of the facility and the range of the thermal scanners. The wells are locked down, alarmed and unmarked except for a telephone number.

Other notes

Only certain areas of the facility have locked racks; racks in other areas are locked with programmable cylinders.

Security guards are not armed, and there is no training for active shooters. Serious breaches call for police intervention. In other instances, security will address the problem and note the incident. Violators can be ejected and banned from the workplace.

Interview 4

SNAPSHOT	
Company revenues	$25-$100 million
Individual interviewed	Head of security
Industry	Colocation
Budget dedicated to security	~6%
Region	Europe
Facility type	Colocation

This colo operator provides security and manages access for four data centers. The facilities have very different threat matrixes because they are sited in very different locations. However, only customers can access IT cages. The facility reports no incidents in the last 5 years. They also build bespoke facilities in which the customers dictate security measures. Security staff is provided by a specialist vendor working to a service agreement with performance measures.

Perimeter

Despite operating in varied environments, the company's data centers all include perimeter fences. They are in the process of evaluating and upgrading perimeter security at two of these facilities, in one case because of nearby construction. They are also adding CCTV at this site.

Vehicles are detained in a vehicle trap and monitored by unarmed on-site security staff using CCTV before being granted access. Actual guard numbers are dictated by the size of the site and any specific customer requirement, but generally two guards are on duty 24/7. The buildings are marked.

Interior

The facilities include a variety of interior technologies, including iris and fingerprint scans, badge readers, badge readers with PIN, proximity readers, man traps (with volumetric sensing) and intruder detection via infrared cameras.

Policies

The colocation company works with a security vendor, which has helped them develop a hierarchy of security policies and documents, including:

- Security strategy document that explains their approach to security management.
- Physical security policy.
- Information security policy.

Interview 4 *(continued)*

- Security manual that details roles and responsibilities applicable to all sites and includes site-specific annexes.
- Guard assignment instructions.

Only pre-announced/authorized visitors are allowed, with their ID verified before registering in the visitor system. The system sends an automated email to on-site training, with an invitation to do a knowledge check.

Visitors must be escorted at all times by their host or another approved cardholder. Trusted regular vendors who have completed site induction training are allowed to work unescorted. Others are escorted. Outside computers, tablets or removable storage devices are allowed as dictated by customer requirements within customer spaces.

Physical access to the data center is approved by the site manager, with customers approving access for their dedicated spaces.

The colo reviews access permissions annually with the customer and more frequently if specified. Access is revoked when the colo is notified and the user is deleted from the system after 6 months.

The colo has policies and guidance for contravention of data center rules but in practice they are not enforced robustly with customers.

Biggest risk

Customers sharing access cards. Each customer is issued 10 cards and through random checks, the colo has discovered some instances of sharing. The problem is usually administrative.

Other notes

Guards escalate any intruder-type incidents to police authorities, and there are no specific policies for an active shooter scenario.

Customer cages have very small openings that must be balanced for air flow; these cages are made of higher grades of steel at customer request.

The company is examining video analytics, which allows tracking using CCTV. The technology would provide faster response times than guards and would be less expensive.

Interview 5

SNAPSHOT	
Company revenues	$25-$100 million
Individual interviewed	Delivery Analyst (Product owner/specialist)
Industry	Financial
Budget dedicated to security	5%
Region	Europe
Facility type	Multiple

This European financial services firm operates multiple facilities. Each facility employs similar strategies, technologies and policies, customized to meet different perceived threats at each location. A colocation operator provides perimeter security at one site. The few reported incidents include lost motorists asking for directions and policy violations.

Perimeter

A security team comprising both company employees and a third-party specialist company controls site access through a staffed gate with a vehicle trap. The building itself is anonymous and protected by a fence and either a canal or berms. Beyond those barriers are landscapes that include sand, trees and bushes, plus an additional small wall. Entries include special locks, and reinforced glass adds to the building security. Vehicles are not inspected.

The within-fence freight vestibule includes a badge reader, and the loading dock has double door with yet another badge reader.

Interior

Visitors must pass through four steps inside the fenced perimeter. There is a badge reader to enter the perimeter, a badge reader to enter the building, security staff guarding the data center space, and a man trap with cameras and a biometric recognition option.

Policies

Access for visitors must be arranged with security 24 hours in advance. When visitors arrive at the data center, they must provide government identification to security guards, who then issue a temporary pass.

Vendor employees are screened according to overall agreements with suppliers, who also perform background checks. Most of these individuals are escorted at all times, but some have higher levels of access and might have their own badges. In these instances, security opens the cabinet and leaves. Technicians can use computers — but not flash drives — on crash carts as described in facility policies.

The facility does not accept unscheduled deliveries.

Interview 5
(continued)

Security guards are empowered to intervene in cases of misconduct, but for other situations they are told to call authorities.

Biggest risk

High-power intrusion, with military equipment. Other than that, the firm is more concerned by the prospect of hacking.

Other notes

The facility holds regular fire evacuation tests.

No concerns about active shooters. The perimeter might have some vulnerability, but the glass shield and building features will protect the facility and its occupants.

Interview 6

SNAPSHOT	
Company revenues	$100-$500 million
Individual interviewed	Datacenter Facilities/Operations
Industry	Pharmaceuticals/Healthcare
Budget dedicated to security	~8%
Region	North America
Facility type	Dedicated production and nonproduction data centers

This North American healthcare organization operates numerous facilities, including many that offer patient services. Security issues at one facility in the last 5 years included locals who scaled fences seeking shortcuts. System-wide, individuals sometimes mistake IT facilities for hospitals.

Perimeter

This pharmaceutical/healthcare provider uses an unarmed contracted service to provide security for its facilities, with the production sites including perimeter fences. Both types of sites include landscape features, bollards and other barriers. There are two remotely monitored and activated gates at all site, with one for fire response. The gates are controlled by a badge system and call box. There are some signs indicating the name of the enterprise but not the building function. As a result, individuals sometimes approach the facilities, seeking patient services.

The loading dock includes roll-up doors monitored by cameras; contacts are controlled by badge readers. Packages must pass through multiple doors to access the critical space.

Interior

Technologies employed on the site include:

- CCTV throughout the site.
- Handheld radios.
- Anti-piggybacking systems.
- Dual authentication.
- Call boxes.
- Badge reader.
- Badge reader with PIN.
- Cameras.

Policies

When a person is screened and presents their credentials, security calls the organization's Network Operations Center to validate their

Interview 6 *(continued)*

entry. Visitors can access data centers only if pre-approved and must have an escort.

Vendors require a validated service ticket and can work unescorted in the areas they are assigned. Vendors do not get permanent badges; rather, in exchange for government-issued ID, they are given a one-day, returnable badge. Regular vendors can be added to a pre-approved access list.

Security can access about 75% of the facility but, for safety reasons, are not permitted in some critical power spaces. Internal IT customers can access only spaces that are in their scope of work, with white-listed data center staff having all access badges and keys. Service vendors are not allowed to switch or manipulate equipment.

Other staff carry appropriate credentials issued on a 90-day “use it or lose it” basis, with all badges and passes subject to an annual audit per Sarbanes-Oxley Act requirements.

Computers, tablets or removable storage devices are monitored and/or restricted but allowed on an honor system if required to complete the job. The company has policies that minimize the use of personal USB devices.

Penalties for policy violations depend on the severity of the infraction. Usually a “hand slap” is enough, but employees can be terminated for severe or repeated infractions.

The facility does not normally accept packages, but in actual practice, acceptance depends on what is being delivered and whether staff is available to assist at the time.

Biggest risk

Network breaches, trusted intruder, attempts on the building management system and cybersecurity concerns.

Other notes

The company provides annual active shooter training and drills (barricade, run and engage)

Pan-tilt cameras in place, with some infrared. The company monitors critical spaces such as chiller rooms for safety.

The facility also monitors all EPO buttons and critical facility areas.

Interview 7

SNAPSHOT	
Company revenues	>$1 billion
Individual interviewed	Datacenter Facilities/Operations
Industry	Financial Services
Budget dedicated to security	Unknown
Region	North America
Facility type	Dedicated, mixed-use and colocation

This North American financial services company operates a wide variety of facility types. On a site-dependent basis, it employs entire range of common security measures, including armed security at some facilities. The company has experienced no incidents in the past 5 years.

Perimeter

Visitors to this company's data center sites must first pass through a staff gate and vehicle inspections before entering the site. The sites are also protected by fences and bollards, and security operates a vehicle trap at some sites.

Interior

The data center deploys combinations of recognition and monitoring technologies, including biometrics, badge readers, PINs, proximity readers, man traps, freight vestibules and cameras to control access to white spaces and other sensitive areas in the facility.

Policies

Security guards are provided by a third-party specialist that reports to the organization through the Corporate Properties division. The data center owner does not allow tours in any of its data centers, which limits the number of visitors. All others must be approved by data center management, with access reviewed daily and revoked on a weekly basis, if needed.

Vendors are escorted at all times, with the use of outside computers, tablets or removable storage devices restricted to work as required. Any media-bearing devices that go in the data center do not leave the facility and are securely destroyed. Access to racks is provided by the data center team at time of need.

The facility does not accept unscheduled deliveries; all packages are scanned.

Penalties for policy violations include removal and ejection from the site and lifetime bans, depending on the infraction.

Interview 7
(continued)

Biggest risk

Vehicular impact.

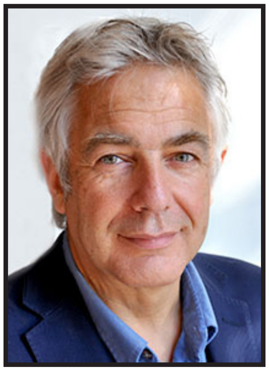
Other notes

Active shooter preparations include lockdown procedures and bunker-in-place drills.

Uptime Institute® | INTELLIGENCE

ABOUT THE AUTHORS

Kevin Heslin is Chief Editor and Director of Ancillary Projects, Uptime Institute. Kevin served as editor of The Uptime Institute Journal, where he authored and co-authored numerous papers, including case studies involving Uptime Institute Tier-certified facilities. Kevin has had a more than 30-year career examining energy and sustainability issues from the end-user perspective. In that regard, he has worked in academic, nonprofit and standards organizations, in addition to serving as editor of various print publications. Contact: kheslin@uptimeinstitute.com



Andy Lawrence is Uptime Institute's Executive Director of Research. Mr. Lawrence has built his career focusing on innovative new solutions, emerging technologies, and opportunities found at the intersection of IT and infrastructure. Contact: alawrence@uptimeinstitute.com

ABOUT UPTIME INSTITUTE

Uptime Institute is an unbiased advisory organization focused on improving the performance, efficiency and reliability of business critical infrastructure through innovation, collaboration and independent certifications. Uptime Institute serves all stakeholders responsible for IT service availability through industry leading standards, education, peer-to-peer networking, consulting and award programs delivered to enterprise organizations and third-party operators, manufacturers and providers. Uptime Institute is recognized globally for the creation and administration of the Tier Standards and Certifications for Data Center Design, Construction and Operations, along with its Management & Operations (M&O) Stamp of Approval, FORCSS® methodology and Efficient IT Stamp of Approval.

Uptime Institute – The Global Data Center Authority®, a division of The 451 Group, has office locations in the US, Mexico, Costa Rica, Brazil, UK, Spain, UAE, Russia, Taiwan, Singapore and Malaysia. Visit uptimeinstitute.com for more information.

All general queries:
Uptime Institute
5470 Shilshole Avenue NW, Suite 500
Seattle, WA 98107 USA
+1 206 783 0510
info@uptimeinstitute.com