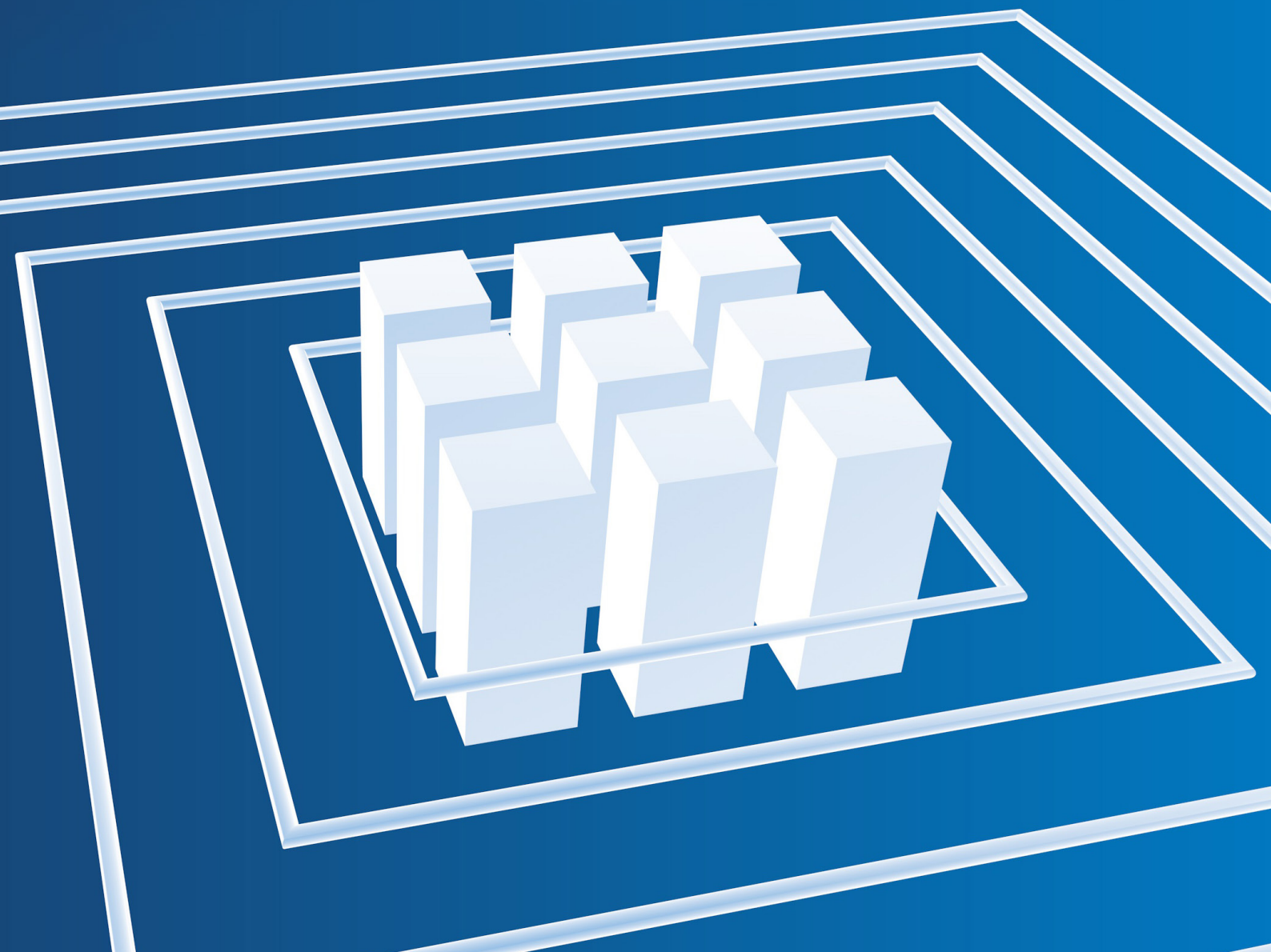


**ANIXTER**<sup>®</sup>

GLOBAL TECHNOLOGY BRIEFING

# RISK MANAGEMENT BEST PRACTICES



# CONTENTS

---

<b>4</b>	EXECUTIVE SUMMARY
<b>5</b>	INTRODUCTION
<b>7</b>	THE RAPID RISE OF THE DATA CENTER
<b>10</b>	RISK IN THE DATA CENTER ENVIRONMENT
<b>12</b>	THE COST OF SECURITY VS. RISK
<b>16</b>	DECLARE BUDGET OWNERSHIP
<b>18</b>	PROTECTING INFORMATION AND PHYSICAL ASSETS
<b>20</b>	DRIVEN BY COMPLIANCE
<b>22</b>	DESIGN STANDARDS AND BEST PRACTICES
<b>24</b>	A MULTIFACETED STRATEGY FOR PHYSICAL SECURITY
<b>25</b>	MACRO-SEGMENTATION STRATEGY
<b>28</b>	THE SIX LAYERS SUPPORTING THE PHYSICAL SECURITY OF A DATA CENTER
28	Layer 1: Perimeter Defense
31	Layer 2: Clear Zone
34	Layer 3: Facility Façade and Reception Area
36	Layer 4: Hallways, Escorted Areas and Gray Space
38	Layer 5: Data Center Room and White Space
41	Layer 6: Data Center Cabinet
<b>45</b>	CONCLUSION

# FIGURE INDEX

---

**Page 6 Introduction**

Figure 1: Data center security threats

---

**Page 7 The Rapid Rise of the Data Center**

Figure 2: Data center space (m<sup>2</sup> billion) requirement forecast – 2012-2020

**Page 8**

Figure 3: Data center growth drivers

**Page 9**

Figure 4: Data center space (m<sup>2</sup>) growth forecast – in-house, co-location/outsourced and total – 2013-2020

---

**Page 10 Risk in the Data Center Environment**

Figure 5: Physical threats to the data center

---

**Page 13 The Cost of Security vs. the Risk**

Figure 6: Investment vs. Risk

**Page 15**

Figure 7: The rights and wrongs of corporate commitment

---

**Page 16 Declare Budget Ownership**

Figure 8: Budgeting for physical security – meeting different executive requirements

---

**Page 21 Driven by Compliance**

Figure 9: Notable industry certifications with security standards

Figure 10: The Ideal Conversation with an Auditor

---

**Page 28 The Six Layers Supporting the Physical Security of a Data Center**

Figure 11: Layer 1: Perimeter Defense

**Page 31**

Figure 12: Layer 2: Clear Zone

**Page 34**

Figure 13: Layer 3: Facility Façade and Reception Area

**Page 36**

Figure 14: Layer 4: Hallways, Escorted Areas and Gray Space

**Page 38**

Figure 15: Layer 5: Data Center Room and White Space

**Page 41**

Figure 16: Layer 6: Data Center Cabinet

# EXECUTIVE SUMMARY

---

This report identifies how the rapid rise of the data center is leading to an increased risk of theft, sabotage and corporate misconduct. However, many data center operators focus solely on logical security, ignoring physical security and its potential threats. This type of thinking leads to vulnerabilities in a data center's security and increases its exposure to unnecessary risk.

Balancing physical security with logical security is the only way to protect a data center. This paper analyzes the cost vs. risk of data center security, the importance of physically protecting assets and the value of declaring security budget ownership. Driven by industry regulations, design standards and best practices, physical security in the data center is as important of an investment as the latest firewalls and cyber security protocols.

Throughout the chapters, the paper lays out the steps to create an effective multifaceted physical security strategy that focuses on implementing a six layered physical security approach.

Finally, this paper examines the need for data center physical security and the risks to organizations that don't properly protect its critical data. It also sets forth a series of standards and best practices for protecting data centers at six different layers.

The information presented in this paper is for informational purposes only and shall not be considered technical advice. Readers should seek appropriate independent professional advice prior to relying on, or entering into, any commitment based on material published here, which material is purely published for reference purposes alone.

# INTRODUCTION

---

Whether it's for business or education, entertainment or shopping, nearly every financial transaction, phone call or text, movie download or Internet search either now takes place or is recorded in a data center. With nearly everyone's professional and personal lives dependent upon a healthy ecosystem of data centers, it is only natural that data centers are now targeted by thieves, spies and others maliciously seeking to cause damage or to steal the information contained within a data center.

## Data Breaches are Universal

As data centers have increased in importance, data breaches have become nearly universal. A data breach has happened at each of the 314 companies surveyed in a Ponemon Institute study ("*2014 Cost of Data Breach Study: Global Analysis*") with those breaches ranging from over 2,000 records to "mega breaches" affecting well over 100,000 records.

Never before has a data center breach been more damaging to the future of an organization. As the risk has risen, a growing array of sophisticated threats continues to emerge designed to penetrate data center defenses.

### SECURITY BREACH FACTS

---

- › The average cost of a data breach is \$3.5 million. Not developing or adhering to proper protocols has proved very damaging, as 39 percent of all breaches are a result of negligence.
- › Malicious attacks are on the rise and threaten to supersede negligence as the most common cause of data center breaches.
- › Despite these costs, data center security professionals report only being allocated, on average, 50 percent of the budget that they believe their organizations require.

Source: Ponemon Institute 2014 Cost of Data Breach Study: Global Analysis

## Physical Security: The True Bedrock of Data Security

Data center security is typically thought of as a logical security issue – the use of firewalls, intrusion detection, the hypervisor security protocols in a cloud environment, and other strategies to deter and defend against hackers and other online breaches. However, controlling physical access to the data center is the true bedrock of data security and guards against:

- › Hardware theft
- › A malicious attack on a network port through a virus physically attached
- › Corporate espionage
- › Unauthorized access to sensitive computing and telecom equipment
- › Disgruntled employees and contractors

## Data Center Security

When reading through this report, ask the following questions:

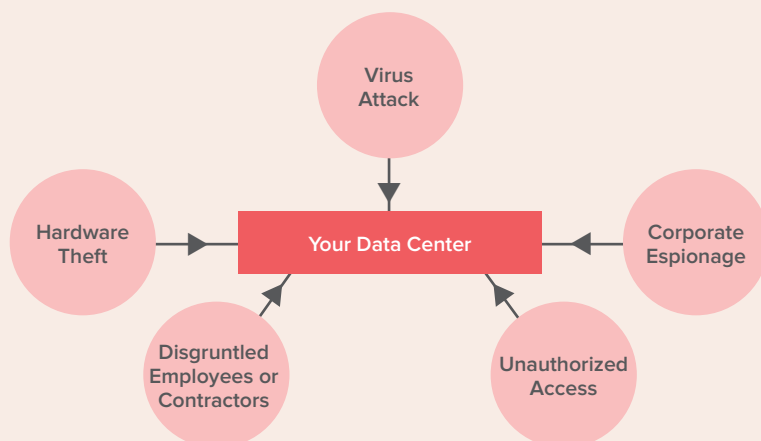
- › Whom in the organization is ultimately responsible for the physical security in the data center?
- › What is the physical security strategy?
- › Does the focus on and budget for physical data center security match the risks?
- › Top to bottom, is the organization committed to data center physical security, or is it complacent?
- › What is the weakest link? Is it the cabinet, gray space, visitor tracking or something else?
- › When was the organization's physical security policy and procedures last updated or reviewed?
- › Does the organization regularly test and enforce physical security procedures?
- › What physical security measures are in place to protect the organization's data center?

We've shown some of the generic threats to the physical security of the data center in Figure 1.

## Don't Wait for a Catastrophe

Many organizations are not focused on physical security in the data center, and in the past, have ignored the issues we raise in this report. However, this can be catastrophic for an organization – as well as for the careers of the executives that didn't develop, implement and execute a suitable data center physical security strategy.

**Figure 1: Data center security threats**

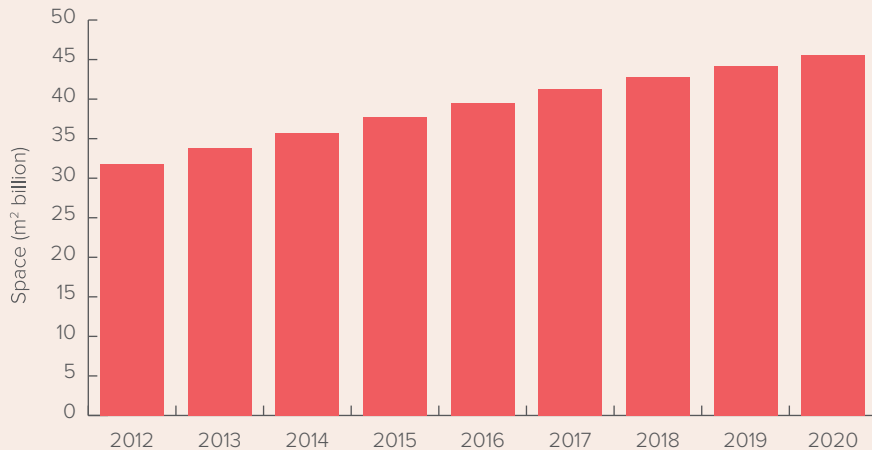


# THE RAPID RISE OF THE DATA CENTER

## Importance and Critical Nature

In a way that would have been unimaginable just 20 years ago, nearly all the key business functions and communications of enterprises, businesses and government agencies are now occurring in data centers, which host the information and applications that an organization uses as the backbone to serve its customers. It frequently contains all the organization's communications, emails, records, financial activities and customer lists used to serve customers, employees, partners and other stakeholders. DCD's global data center market overview and forecasts 2014-2020 shows a continuous rise in the requirement for data center space (see Figure 2).

**Figure 2: Data center space (m<sup>2</sup> billion) requirement forecast – 2012-2020**



1 meter = 3.28 feet

Source: DCD Global data center market overview and forecasts 2015-2020

## Impact of Failure

This increased leveraging of technology allows for far greater productivity, efficiency, scalability and speed than has ever been enjoyed before. The positive attributes of the rise of the data center have a counterpoint: the disturbing specter of potential failure. A security breach could have a devastating impact to an organization if something knocks it offline. Such a breach could have consequences beyond just the organization that is directly affected. Imagine the economic impact if a major financial institution suddenly could not process customers' financial transactions: local economies, even national and global economies, could be affected.

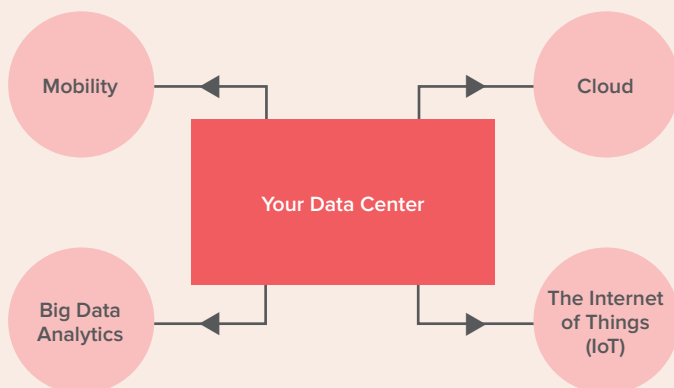
## Mission Critical

Nearly everything an organization needs to accomplish is contingent upon efficient, secure data center operations. The importance of the data center in the achievement of an organization's mission and business goals cannot be overstated.

## Big Data, IoT, Mobility, Cloud: All Growth Trends Continue

Nearly all trends in technology are fueling data center growth (see Figure 3). Big data analytics, the Internet of Things (IoT), the continued explosion of device-driven mobility and cloud computing are just four trends driving growth in the data center. As companies and individuals continue to rely more on technology in nearly every aspect of their lives, it is hard to imagine a future where data centers do not continue to play a central and growing role.

**Figure 3:** Data center growth drivers



## Outsourcing Fuels Data Center Growth

Many companies, especially large enterprises, still prefer the control and security of ownership of their own data centers, and they will continue to do so. The continuing trend of outsourcing non-core operations has led to explosive growth of cloud computing and multitenant data centers. Figure 4 shows DCD's forecast for space requirements by area between 2012 and 2020: it demonstrates the greater need for co-location/outsourced sites than in-house ones.

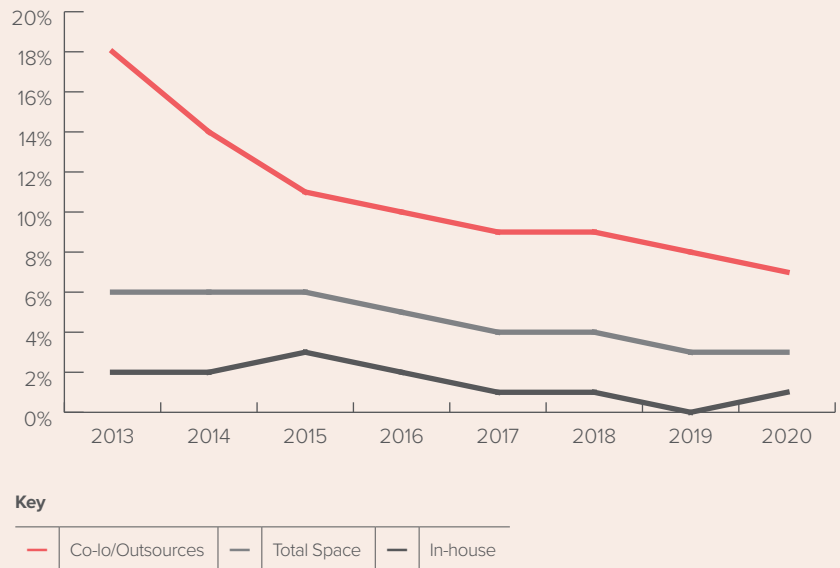
## Cloud Computing Hubs

The two major beneficiaries of the trend toward outsourcing of IT infrastructure have been cloud computing and multitenant data centers. Cloud platforms are hosted in data centers. The most successful cloud providers, Amazon Web Services and Microsoft's Azure and Office 365 SaaS platforms, are building out data center space worldwide at a rapid pace.

## Multitenant Data Centers

Many organizations prefer multitenant data centers where their compute resources are not pooled, but the other aspects of infrastructure and operations (electrical infrastructure, generators, fiber links, security, etc.) are handled by the data center owner on behalf of its tenants.

**Figure 4:** Data center space (m<sup>2</sup>) growth forecast – in-house, co-location/outsourced and total – 2013-2020

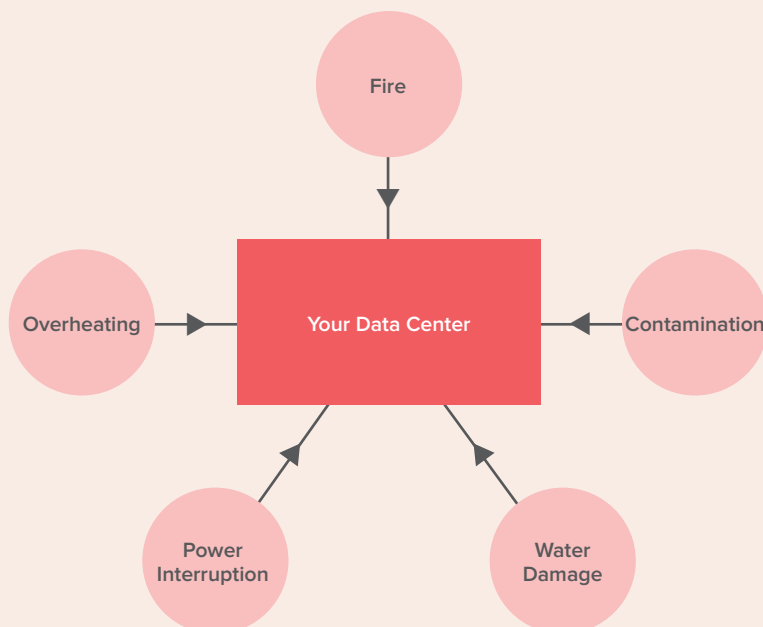


Source: DCD Global data center market overview and forecasts 2015-2020

# RISK IN THE DATA CENTER ENVIRONMENT

There are all kinds of risks in the data center (see Figure 5): fire, contamination (which is why no cardboard is allowed), water damage, power interruption and thermal. As a risk factor, physical security is frequently overlooked, despite its critical importance. As the data center becomes increasingly integral to an organization, the risk of an IT security breach increases and can cause far greater harm than ever before.

**Figure 5:** Physical threats to the data center



## Risk Management

An organization must determine what the risk is of a data breach and use that to determine its investment in risk management. A key component of a risk management plan is the proper tools to establish a solid baseline of defense against potential threats, but equally important is the organizational buy-in needed to managing that risk.

### DID YOU KNOW?

Despite the spotlight on data breaches, security experts agree that only a small fraction of these breaches even become known to the public. Most are handled quietly, particularly in B2B environments where both sides of a business relationship understandably choose to keep the incidents quiet to avoid embarrassment and the appearance of vulnerability, incompetence and mismanagement.

## Security is Everyone's Responsibility

Key stakeholders throughout the company should understand the damage that can be done and demand focus on and adherence to best practices in protecting against potential breaches can cause.

Even though the Chief Information Officer (CIO)/ Chief Information Security Officer (CISO) has frequently been the one to face the firing squad in the case of a data breach, Chief Executive Officer (CEOs) can also lose their jobs if they fail to foster an atmosphere of strict compliance with the best practices of data protection and security. A data center security event can easily become a 'resume-generating' event not just in the executive suite, but among frontline staffers as well.

Technicians, security guards, cleaning staff, operations professionals and others in the data center need to make physical security a team effort.

## Avoiding Data Breaches is Everyone's Job

It is important for everyone in an organization to understand that data breaches are not restricted to hacker incursions into a system. Just a single individual letting down his or her guard in a data center and permitting an unauthorized person access to the IT infrastructure is all it takes for a malicious individual to get access to a server and upload a virus, cut some cords, rip out a server and walk out. Human error, mistakes and failing to follow protocols (assuming best practices are in place) can lead to tremendous damage.

# THE COST OF SECURITY VS. THE RISK

---

The costs of a data breach are significant: a 2014 study by Ponemon Institute found that the average cost of a data breach was \$3.5 million. This damage can take place whether the incursion is via a hacker or via a stolen server. In fact, lost or stolen devices are the number one factor in increasing the per capita cost of a data breach. Logical and physical security must be taken seriously and work in conjunction with one another.

## WHAT WE HEAR

---

Challenges from the various data center stakeholders are:

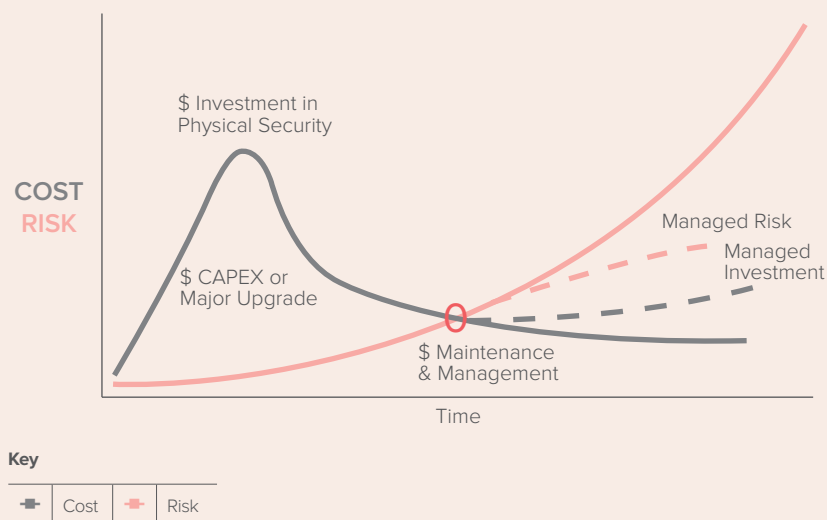
- > Protecting the company's image
- > Achieving regulatory compliance (HIPAA, PCI-DSS, SOX, GLB)
- > Balancing investment in both physical and logical security
- > Staying one step ahead of adversaries with technology
- > Executing policies and procedures specific to the data center

## Investment vs. Risk: Striking a Balance

Physical security deployments are significant investments with the majority of costs incurred up-front. Once installed these security systems are often considered adequate, receiving little to no maintenance post installation. However, as we have discussed risk is continually evolving as equipment nears end-of-life, processes become outdated and the those with malicious intent get more sophisticated.

By building a scalable interoperable security solution, pro-active updates and upgrades are simpler, quicker and more cost effective than complete system revisions, helping you effectively balance the costs of maintaining a robust physical security system with reduced risk of attack and breach (see Figure 6).

Figure 6: Investment vs. Risk



### DON'T BE A STATISTIC

Average organizational cost of data breach was \$3.5M. The number one factor that influenced the cost was lost or stolen devices.

Source: Ponemon Institute 2014 Cost of Data Breach Study: Global Analysis

## Defending Against the Array of Constantly Evolving Logical and Physical Security Threats

Any data center operator, as well as any tenant in a co-location environment, has a need to stay on top of rapidly evolving and growing threats to its security.

### Serious, Smart and Skilled Adversaries

The malicious thieves, corporate spies and revenge-minded vandals executing attacks of all kinds are numerous, relentless and ruthless. The perpetrators may be engaging in corporate espionage, they may be seeking to financially harm an organization or they may simply be maliciously seeking to damage an organization for whatever reason (including just the thrill of it). They may be backed by foreign governments, or they may be competitors, or they may just be common thieves with uncommon skills.

Whoever they are, they can do lasting damage to customers, an organization and careers. An organization must invest in stopping them.

### Establish a Culture of Preventive and Active Security

Security professionals hear of new tactics on nearly a weekly basis, and truthfully, there is reason to be impressed by the creativity and resourcefulness on the other side of the battle. The competition is tough. An organization must take the threat seriously and must commit to the fight.

## Steps You Must Take

### **Create a Battle Plan**

What are the plans and procedures to defend against threats that are increasing in sophistication and complexity?

### **Invest the Time and Be Informed**

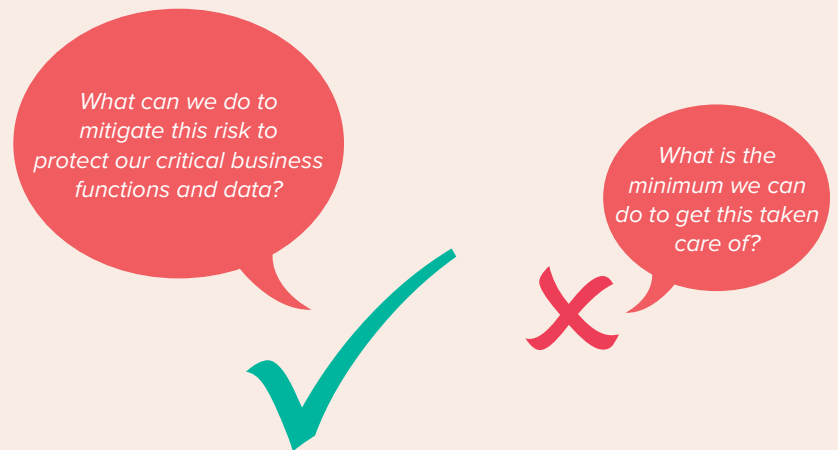
Being properly plugged in with the data center security world should be a priority for an organization. Join some of the active, vibrant communities of security professionals who share the latest threats and ways to overcome them. Attend industry conferences (BICSI, ASIS and DatacenterDynamics) and join, participate, listen, learn and share.

### **Complete Organizational Commitment: Including the Budget**

From the boardroom to the front lines, an organization must have complete buy-in and commitment to the level of security it requires (see Figure 7).

To stay ahead of the risk factors, the strategy must be to exceed the requirements, not to simply accomplish the minimum necessary to hit the marks.

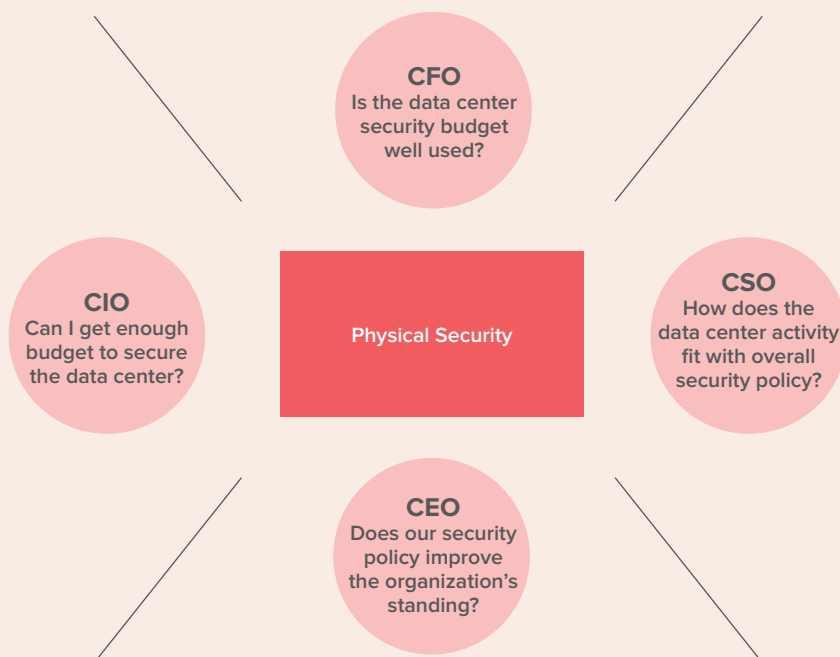
**Figure 7:** The rights and wrongs of corporate commitment



# DECLARE BUDGET OWNERSHIP

Having a substantive budget is not the only issue. The ownership of that budget and the responsibility for it to be wisely used are critical factors. In most organizations, logical security is part of the IT budget. The physical security is not so clear-cut.

**Figure 8:** Budgeting for physical security – meeting different executive requirements



## Cost Analysis to Determine the Budget

Unfortunately, adopting the proper defense posture is not an inexpensive proposition. Surveys of data security professionals show that they believe their budget should be 50 to 100 percent higher. When considering the alternative, allocate the proper resources to protect the data center. The costs of not doing so are just too high of a risk to accept.

### PHYSICAL SECURITY BUDGET CHECK LIST

- > Where does budgetary responsibility lie for the physical security of the data center?
- > What is the annual budget for physical security of the data center?
- > What is the decision making process for this budget? Who is involved?
- > Is the budget focused just on the data center white space or on all six layers of the data center, which are defined on page 28?
- > Is the budget proactive or is it instead more of a patching of weaknesses?
- > How much input is solicited and received throughout the organization?
- > What is the strategy to make sure that the money is used well?
- > Can the physical data center security be scaled as needed?
- > Is there the proper interoperability to keep adding pieces or do systems that don't communicate cause a need to "rip and replace"?

We've captured some of the different views of typical executives in Figure 8.

# PROTECTING INFORMATION AND PHYSICAL ASSETS

---

## The Environment Determines the Protection

The strategy and methodology for protecting the IT infrastructure depends on the business taking place in the organization.

- › A service provider that hosts its entire business platform in the data center in a busy city should rightfully have a very high level of security.
- › An enterprise data center with just a few employees in a rural area where it is easy to monitor who comes and goes may not need a large budget to maintain security.
- › A federal contractor doing work for a high-security agency needs the highest levels of security.
- › A multitenant data center with 80 customers that has employees and contractors coming and going has very specific security needs, particularly in tracking where visitors go within the data center and making sure they cannot access the infrastructure of other tenants.
- › A large company that has a disaster recovery data center that backs up email and other records likely would not require as high an investment.

## What Tier is it?

Uptime Institute and Telecommunications Industry Association (TIA) rate data centers by tier level, from Tier 1 to Tier 4. There are only a handful of Tier 4 data centers in North America. The more mission critical a data center is (and the more importance achieving and maintaining a high tier level is) the higher the protection requirements. Tier levels focus on uptime and securing the primary and backup infrastructure that maximizes uptime is a critical part of achieving a desired tier level.

Even though the Tier Classification System does not prescribe security provisions, physical security risk factors should be addressed in the owner's operational sustainability requirements. The level of security is largely determined by the industry, the criticality of the IT function performed on the site and the owner's policies. For example, a financial institution will typically invest in a level of security exceeding that of an academic institution.

Within the IT infrastructure there are numerous 'best practice' security measures to be taken, regardless of Tier. These include biometric readers, bollards, guard houses, hiding in plain sight, mantraps, re-enforced perimeter fencing, video surveillance, etc. Best practices are critical in reducing the risk exposure of curiosity, mischief, crimes, and accidents. However, best practices should not be confused with Tier requirements.

## Physical Security Plan

A well thought-out, strictly defined physical security plan is necessary when developing and maintaining a strong security stance. Such a plan should cover every aspect of data center security, from designing a system, to having everyday policies on operations, handling visitors, and emergency and disaster response policies.

Security doesn't just happen; it is a result of a process. A well-designed physical security plan is a key part of achieving the desired results.

## Maintaining Sound Policies and Procedures

No matter what the focus of a data center, it is critical to maintain and follow sound policies and procedures. This is part of an overall security plan that balances best practices with a willingness to evolve to properly defend against new threats.

- › Sound policies and best practices support security in a data center.
- › A policy document is a living, breathing thing. Policies are not static. Policies should be frequently reviewed and updated.
- › The logical security strategy should have a physical component to it.
- › Security protocols should be understood by all and followed closely.
- › Complacency must be avoided throughout the organization.
- › Logical security and physical security policies are interrelated and support one another.

# DRIVEN BY COMPLIANCE

---

Security is one of the two key components of compliance, as is uptime demonstrated by the use of redundant systems and best practices for maximum uptime. Many organizations have worked hard to achieve compliance only to lose those hard-earned certifications necessary for operating within their industry. A weakening of an organization's compliance stance can be devastating to its future prospects.

Addressing physical security is complying with regulations and standards. Those who set the standards compliance in various industries have an increasing understanding of how controlling access to a facility helps threats from interfering with the power and telecommunications systems integral to the operation of a data center, along with the data itself.

Compliance standards are unique to individual industries, but share many commonalities. For example, Payment Card Industry Data Security Standard (PCI DSS) certification, which covers the payment card industry, requires a compliant organization to:

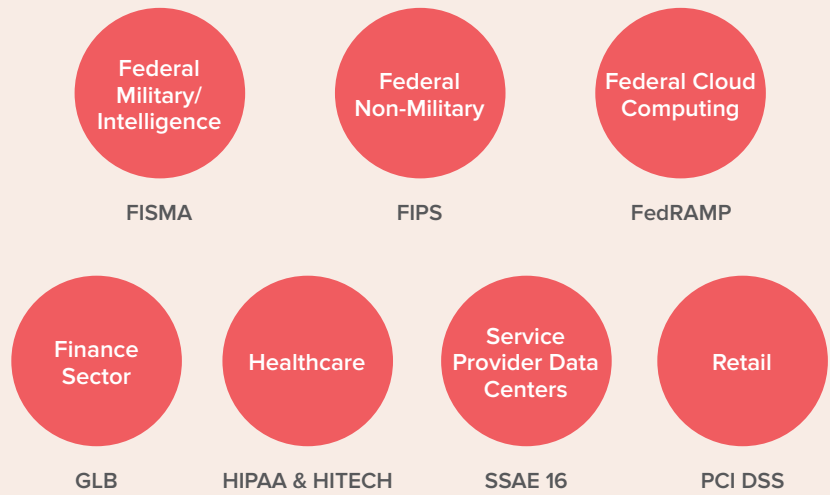
- › Protect stored cardholder data
- › Restrict access to cardholder data by business need to know
- › Identify and authenticate access to system components
- › Restrict physical access to cardholder data
- › Track and monitor all access to network resources and cardholder data
- › Regularly test security systems and processes

These security requirements can be met by physical security protocols and support the need for multiple layers of security as defined in this report.

A layered approach that meets the specific needs of the payment card industry to achieve PCI DSS compliance would include steps welcomed by an auditor evaluating the security stance of organizations seeking compliance with the standards in other industries as well. With the same goal of data protection, it is no surprise that different industries have commonalities in what is required for compliance.

There are many other certifications in a wide range of industries (see Figure 9 for how some apply to different industry sectors). Even though there is significant standards overlap, each individual certification is unique. There are several examples of organizations that lost their critical certifications and have hamstrung their ability to operate in their industry or serve customers in a particular industry. An organization's security stance is an integral part of maintaining compliance and needs to provide sufficient focus and budget to deliver true physical security in the data center.

**Figure 9:** Notable industry certifications with security standards



## The Importance of Auditors

Independent auditors determine if a data center meets proper standards, and that auditing report will usually be universally accepted (see Figure 10 for the ideal conversation a CIO might have). Auditors see different things and interpretation can be a challenge. Having clarity on plans, procedures and protocols minimizes the risk of leaving an organization open to an interpretation issue.

**Figure 10:** The Ideal Conversation with an Auditor

*"Here's our physical security plan. We classify our data center as a critical facility. We have these different rings of security to provide defense in depth. Here are our protocols and procedures. Here's what we do. We're committed to doing things the right way."*

# DESIGN STANDARDS AND BEST PRACTICES

---

Whenever possible, implement key data center design standards. A critical infrastructure approach to physical security for data centers should protect from the facility perimeter to the data center cabinet by leveraging industry standards and best practices.

Proper design and layout of a data center enables the effectiveness of these and the many other systems that provide the attributes and services required of a modern data center. The standards are guidelines that tend to be general, broad and baseline, creating another instance where a comprehensive, strategic approach is more likely to earn the certifications desired.

## Data Center Design and Security Standards

- › **ANSI BICSI 002-1014:** Best practices for data center design
- › **TIA-942:** Sets requirements for telecommunications infrastructure within data centers
- › **Uptime Institute:** Focused on improving the performance, efficiency and reliability of critical business infrastructure
- › **ASIS:** Seeks to advance security standards worldwide
- › **SANS:** Information security best practices and standards
- › **ONVIF:** Focused on network-based physical security product interoperability

A layered approach maximizes the achievement of all necessary certifications. It leverages the insight from all major standards and builds a holistic approach.

Awareness and understanding of these standards is a must for anyone building a data center, whether it be a greenfield build, a conversion of a facility or an upgrade of an existing data center.

Integral to the overall standards of data center design is the understanding that each component of the physical security system meets the standards set by subject matter experts in each area of data center design. These include technological standards for networking infrastructure, physical infrastructure and physical security.

# A MULTIFACETED STRATEGY FOR PHYSICAL SECURITY

---

Given the increasing reliance upon the data center, the harm that can be caused by a security breach and risk inherent in the loss of (or inability to earn) necessary certifications and compliance standards can be crippling. As a result, DatacenterDynamics and Anixter have partnered on a project to properly define the expanded best practices required for secure, compliant data center operations in the current environment.

This technology report defines the six key layers of a holistic data center's "defense in depth" physical security strategy.

1. Data center cabinet
2. Data center room and white space
3. Hallways, escorted areas and gray space
4. Facility façade and reception area
5. Clear zone
6. Perimeter defense

Some data centers are not designed to support all six layers and some layers may be combined. For instance, a smaller data center may not have a significant clear zone, with the perimeter defense leading immediately to the facility façade and reception area. Additionally, a multitenant data center with significant foot traffic may have different security needs than an enterprise data center, but the proper physical security protocols and best practices should be implemented wherever possible.

# MACRO- SEGMENTATION STRATEGY

---

Logical security frequently relies upon the concept of micro-segmentation, which creates barriers within a virtual environment to keep someone who has penetrated the system contained. There are barriers placed throughout the system to keep them from moving from virtual machine to virtual machine. When properly designed and implemented, it keeps a hacker contained while also creating alerts to inform those monitoring the system of any potential incursion.

The six layers of physical security defined here support a macro-segmentation strategy for physically defending a data center. Like a virtual micro-segmentation strategy, a physical macro-segmentation strategy should strive to not limit the performance of the data center, in this instance, by making a data center overly difficult and time-consuming to visit or navigate.

**Six Layers Supporting 5 D's:** A physical macro-segmentation strategy seeks to limit the damage of a threat by supporting the 5 D's of perimeter security.

1. Deter
2. Detect
3. Delay
4. Defend
5. Deny

A layered physical security approach provides a strategic series of obstacles to protect against a potential physical incursion of a data center, making it increasingly difficult to gain access to the mission-critical data.

## The Building Blocks

Key industry protocols leveraged as baseline standards for the six layers include BICSI, TIA, ASIS and ONVIF. These and other standards were critical in the development of a holistic physical security approach designed to protect the data center.

## The Necessity of Interoperability

The entire ecosystem that serves the data center physical security market must do an increasingly better job of providing interoperable solutions that support standards-based open architectures. A multifaceted, layered approach will have different components provided by best-of-breed manufacturers. Systems that don't integrate with one another are an impediment to the mission of keeping data centers secure.

Network-based solutions are clearly the future of data center security and disparate systems that do not talk to one another will be left behind. Decision-makers must not tolerate inefficiencies in systems management. Proprietary manufacturing can lead to a dead end for the end-user seeking a comprehensive solution from multiple providers. Open-architecture solutions enable a scalable, flexible, long-term security solution and put the end-user in control.

Physical security systems have reached a significant point in their evolution. Formerly, manufacturers built proprietary systems without regard to integration with others. Limited interoperability then emerged as manufacturers began building their own ecosystem of partners; however, with volatility in the physical security market, these solutions can put end-users' security platforms at risk. The industry has now grown to the point that a true open architecture has emerged to support standardized communication between network-based physical security products, regardless of manufacturer.

## True Scalability

True, standards-based open systems and open architectures allow end-users and their integration partners to be in control of the system. They can confidently scale and build in forward compatibility as they grow into their future needs. With the addition of physical security standards, end-users can now build end-to-end standards-based physical security solutions to protect and scale with their critical data center environment.

The graphic represented below shows some of the industry standards that support a true open architecture.

Networking Architecture Standards	     
Infrastructure Standards	    
Physical Security Standards	    

**An Open Systems Challenge:** Manufacturers must be truly involved in open standards development, and not just give the appearance of compliance in order to optimize sales. As an end-user, the flexibility, efficiency and scalability of a security systems depends upon a true commitment to open architecture from the technology partners. Technology partners should be asked how they are investing time, energy and resources to continue the development of open physical security industry standards. This is a good indicator of the type of technology partner being selected as part of a data center physical security strategy.

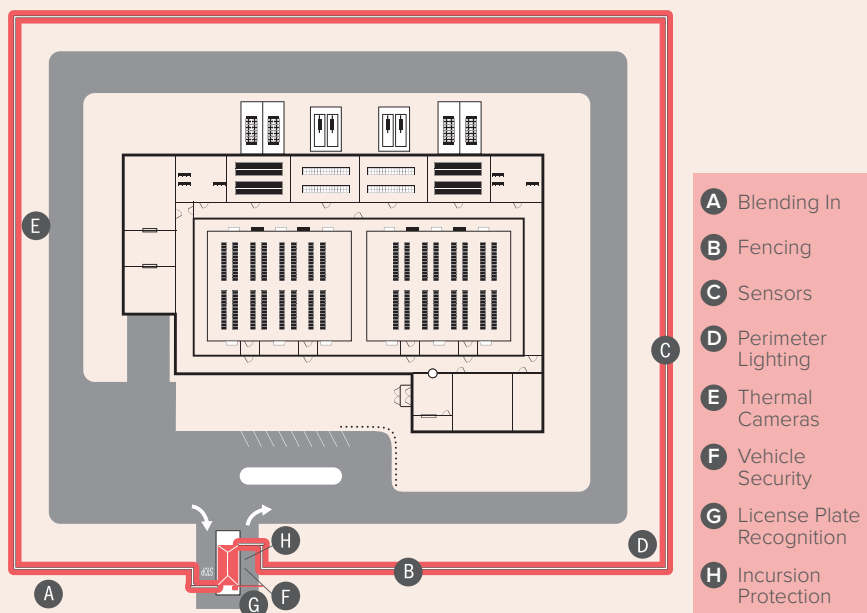
An effective, layered approach requires all systems to work in a cohesive manner. Interoperability has become an absolute requirement in the design and operation of a data center security strategy and manufacturers, integrators and other suppliers that do not focus on the need for interoperability will be left behind.

# THE SIX LAYERS SUPPORTING THE PHYSICAL SECURITY OF A DATA CENTER

## LAYER 1: PERIMETER DEFENSE

Recall the six layers of data center physical security should be based on the 5 D's of deter, detect, delay, defend and deny. The first layer - perimeter defense - controls authorized and unauthorized access to the data center's property. When properly implemented, the perimeter defense layer can reduce the overall cost of a data center facility's security system and improve the effectiveness of the security plan.

Figure 11: Layer 1: Perimeter Defense



## Crime Prevention Through Environmental Design

The concept of crime prevention through environmental design (CPTED) is a philosophy that encourages the use of architectural design to support security.

CPTED is a philosophy of territorial control, where natural surveillance and access control are used. Think of berms, big boulders, clear views without trees or brush in the way for natural surveillance and other methods of natural access control.

This not only allows for better monitoring, but also serves as a deterrent as well. It supports the perimeter defense and frequently does so at a low cost.

## Blending In

Most data centers do not have signs that indicate the nature of the business that takes place. Enterprises have no reason to attract attention to the data center and multitenant data centers' clients frequently feel the same way.

## Fencing: The first line of facility protection

For many data centers, a relatively simple fence that separates a facility from the environment may be suitable. However, for high-security data center installations, numerous fencing options are worthy of consideration.

## Sensors for Security

Sensors for perimeter intrusion systems use special cable media (copper and fiber optic) and electronics to sense vibrations and disturbances to identify if there is an intruder attempting to compromise the perimeter defense. These solutions can be deployed as zones in fences, walls and underground applications. They can also seamlessly integrate with various physical security subsystems to provide complete situational awareness.

## Perimeter Lighting

Lighting is an important part of a data center's perimeter security intrusion detection system. Not only does it provide improved visual coverage for security personnel and video surveillance cameras, but it also improves the effectiveness of the overall security system. Most perimeter lighting applications have turned to infrared (IR) and white-light LED lighting solutions in place of traditional outdoor lighting such as low-pressure sodium, halogen and metal halide.

IR LED lighting solutions can be used in covert perimeter applications covering long distances. White-light LED has multiple functions, such as providing light for video surveillance cameras to identify intruders, as a part of a CPTED strategy as deterrent lighting, or for general area illumination for the safety of site personnel.

## Thermal Cameras

The perimeter of the facility can also be monitored with thermal cameras. In many cases, only the main entry point will be well-lit. A thermal camera allows confirmation of someone outside the facility even in complete darkness by detecting heat signatures emitted by objects. Thermal cameras can also be used with video analytics (perimeter tripwire) and other intrusion detection sensors to create a strong perimeter defense.

## Vehicle Security Station

The key entry point for many data centers is a manned security booth at a vehicle entry point and/or a camera and audio system that allows an internal security desk to communicate with those in vehicles as they go through a checkpoint. Only authorized visitors are allowed and tools such as mirrors and bomb-sniffing dogs are frequently used at higher-security facilities. A motorized operating gate is an additional option for both deterrence and protection.

As a vehicle approaches a data center's guard station, long-range badge readers can determine the identity and level of clearance of someone driving to a gate and assist the security personnel in identifying those occupying the vehicle.

## License Plate Recognition (LPR)

Specialized infrared-sensitive LPR cameras are capable of capturing the license plates of even fast moving vehicles in ambient light levels from bright sunlight to complete darkness. The license plate numbers are then converted into a computer-readable format and compared with a database of vehicle registration numbers. This allows an assurance that an authorized user is in an authorized car, allowing a guard to quickly validate this person or to discover why a non-authorized person is approaching the facility.

## Incursion Protection

Wedge barriers that rise up out of the ground to create an obstruction to potential intruders and crash-proof fencing may be used to guard against vehicles engaged in an incursion. The outer perimeter is another area where policy, video, deterrence, protection and active monitoring create a secure environment.

## LAYER 2: CLEAR ZONE

The clear zone is extremely important. After getting through the perimeter, the threat may have access to critical electrical and mechanical areas, such as the primary power plant and power wires running into the facility, or other backup areas, such as generators and fuel tanks. The clear zone also contains equipment loading docks and secondary entry points into the facility.

### Video Surveillance

Video monitoring is a key part of data center access control. It can serve as a deterrent, as a monitoring tool and as a way to review an incident. An active video monitoring system can guard against “tailgating,” and video monitoring will help enforce security policy.

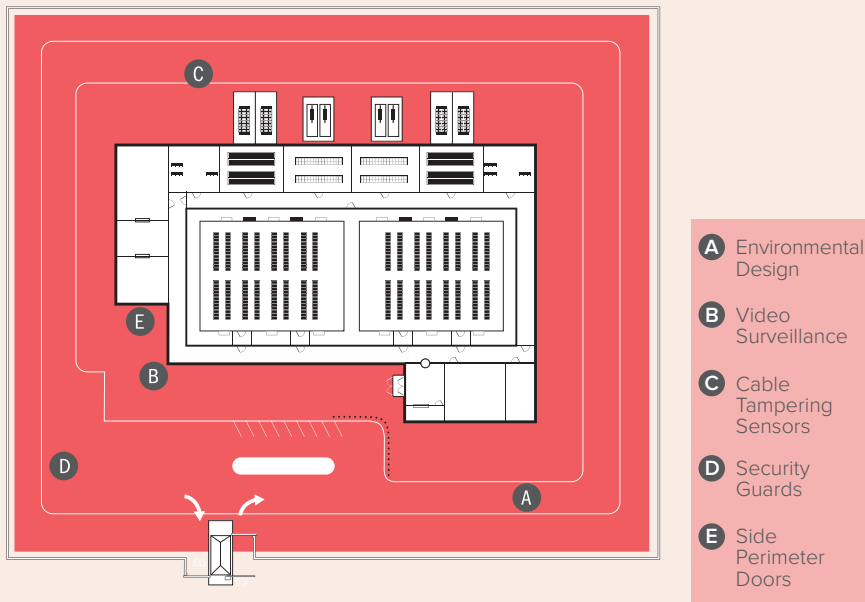
Video has uses in every layer of a data center’s defense, and defending the clear zone is no different. In the clear zone, the primary goal is to identify individuals and monitor restricted areas. Video surveillance is key to keeping the clear zone secure.

#### DID YOU KNOW?

To enhance the performance of the video surveillance system, a best practice is to use LED lighting in the clear zone in place of low-pressure sodium or mercury vapor light. LED lighting offers numerous benefits from energy savings to reduced maintenance. LED lighting also provides superior lighting conditions allowing cameras to deliver high quality nighttime images. Here are some of the major benefits of using LED lighting with video surveillance:

- > Increases high-resolution camera performance in low-light
- > Reduces bandwidth consuming video noise during low-light scenes
- > Provides better color rendering vs. traditional lighting (e.g. low-pressure lights produce a monochromatic light that impact color rendering)
- > LED lighting is offered in both infrared (IR) and white light options

Figure 12: Layer 2: Clear Zone



## Video Strategy Supporting Security Protocols

There are several strategies to support security protocols with video including the following:

- › A focus on power sources. Who is in proximity of the power infrastructure, fuel tanks, loading areas and generators within the clear zone?
- › Use high-resolution 180° degree cameras. Pan, tilt and zoom cameras don't provide constant coverage.
- › Detection and identification of people within the clear zone. 20 to 80 pixels-per-foot cameras are required to see who is approaching the facility.
- › Get complete coverage of the clear zone. Cameras may be required from the building looking out and the perimeter looking in to ensure there is complete coverage and no dead zones.

## Determining the Optimal Camera Resolution

Paying attention to optimal camera resolution makes sure there is proper image detail (pixel density) in everyday and worst case scenarios. Many times, it seems easy to pick a high-resolution camera and feel comfortable that it will do the job. That's not necessarily the case. Too high of a resolution camera can be overkill for the application and create unnecessary stress on the network by creating excessive bandwidth and storage requirements and costs. On the other hand, too low of a resolution camera can be the difference in being able to properly identify a potential threat or suspicious activity. So, what is the best way to optimize camera resolution? Here are some simple steps to follow to help optimize camera resolutions for data center video applications:

- › Determine operation requirement. What is the 'everyday' use scenario? What is the 'worst case' use scenario?
- › Work with technology partners to help determine the pixel density requirement to meet the operational requirements.
- › Be aware that complex issues such as lighting, optics, compression and others can impact image quality.
- › Leverage the pixel counting tools available in most network cameras to validate pixel density once a camera is installed.

When developing a video strategy, it is important to remember that video is only as good as the people who are watching it. How vigilant are they going to be after they've been on the job a while? How alert and focused is the overnight security personnel at 4 a.m.? Those realities are fueling the growth of video analytics.

Video analytics can be used at different layers. Uses for video analytics in the clear zone include the following:

- › Alerts in case individuals are loitering in monitored areas based on suspicious movement.
- › Object classification provides alerts based on the type of object (person, vehicle, animal, etc.) detected.
- › Direction flow provides alerts based on the direction of a moving object.
- › Object added/removed alerts if an object is added or removed from a predefined area.
- › Motion tracking follows a moving object across the cameras view.

### A SECURITY GUARD REALITY CHECK

Security guards may have varying degrees of experience and training. If the security staff is outsourced, that is another level of control over the guards that isn't available. Given the varying quality of security guards, company policies and procedures are paramount, as is the buy-in of everyone in the facility to support the security protocols of the data center.

## Cable Tampering Sensors

In high-security data center applications, it is important to deploy physical intrusion detection sensors that protect critical telecommunications and power transmission cabling infrastructure throughout the various layers of the data center's physical security strategy. Sensors should be deployed in parallel within a network conduit, embedded in a carrier or used to physically protect optical networks from an individual attempting to compromise the infrastructure. This is done by providing a security alarm to detect a physical intrusion or the tapping of information. These systems can also aid in identifying if an intrusion in the network is a physical or logical attack.

## Side Perimeter Doors

Another element of clear zone security is protecting non-main doors from attack. As a physical barrier, a door with a single point of latching into the frame is easy to defeat. Higher security, multipoint locking systems are available. They add latch points on the top, bottom, middle and hinge sides, making the door invulnerable to physical attack from outside.

## Use of Controlled Key Systems

In a restricted, high-security key system, key blanks are under control of the manufacturer. Under no circumstance can they be copied anywhere else and the distribution and management is strictly controlled.

## LAYER 3: FACILITY FAÇADE AND RECEPTION AREA

### Commit to Visitor Management

Visitor control starts at the reception area and sets the tone for the data center. Visitor control is becoming a larger part of achieving compliance. PCI DSS, a key financial industry certification, is among the standards requiring strict visitor controls. In a PCI DSS compliant facility, a visitor needs to be clearly identified via a visitor badge.

A visitor badge is not merely a generic badge; rather, it should be created with a photo badging system onsite for visitors. The visitor badge should additionally have an expiration date and time. This badge clearly indicates who the person is and how long they are permitted to be in the facility. A good practice is to fully integrate the visitor management software with the access control system. This gives security personnel one place to manage both visitor and employees.

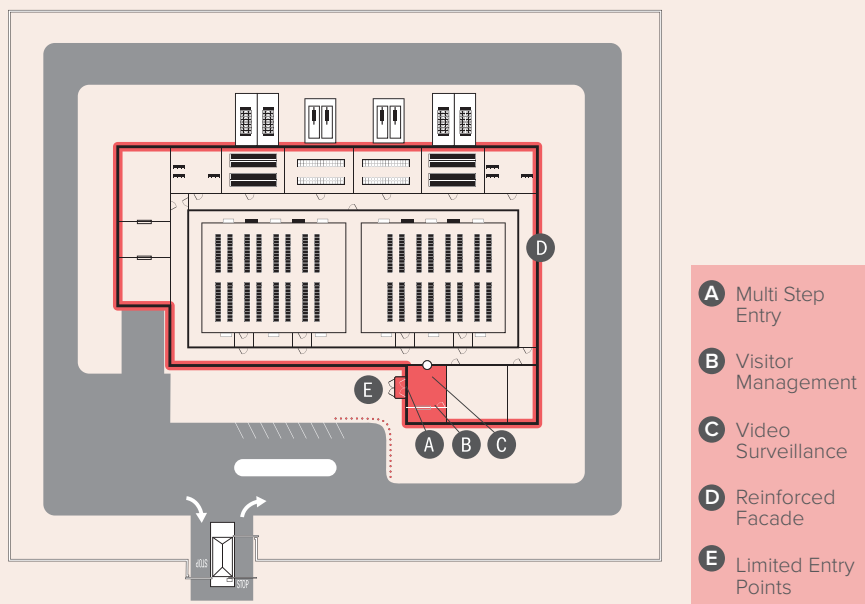
### Complacency is the Enemy of Security

The security staff in the reception area must understand that just because a contractor or visitor has been through the process before, it doesn't mean that the process can be relaxed in any way. Complacency should never set in. Complacency is a breeding ground for a security breach, allowing even the most sophisticated security apparatus to be defeated.

#### UNDERSTANDING THE ENVIRONMENT

Frequently, sunlight permeates a glassy visitor area. As a result, there may be a need for wide dynamic range (WDR) cameras. A standard camera without WDR cannot compensate for the dark inside of a building and bright sunlight light coming into reception area; WDR cameras adjust and compensate for both bright light and dark areas.

**Figure 13:** Layer 3: Facility Façade and Reception Area



## Interoperability Keys Guest Verification

An access control system can integrate and sync up with HR management systems such as Oracle PeopleSoft in order to verify the to-the-minute employment or contracting status of the visitor. This avoids the potential actions of a disgruntled employee immediately following termination.

## Multistep Entry

Ideally, a visitor would be badged in before the reception area. A video camera near a card reader can see who that person is and where he or she is coming into the facility. An intercom system is used to facilitate communication and verify that someone has business with the facility. The intercom system can utilize VoIP technology and become a part of the communications infrastructure.

## Video Surveillance

Like the previous areas of the data center, video is critical as visitors approach and enter the building. High-resolution cameras are recommended to provide clear identification of who the person is coming into the facility. Also, if the video and access control systems are integrated, a positive identification and verifiable record of entry is provided for each instance.

## Everyone's Responsibility

An adherence to policies and procedures is extremely important when allowing admittance to the data center. It starts with the security staff and receptionist, but following best practices as laid out by the organizational security policy by all employees in the data center is required at this critical stage of the security process.

## LAYER 4: HALLWAYS, ESCORTED AREAS AND GRAY SPACE

Most data centers have significant focus on the white space of the data center room, but the gray space, hallways and escorted areas that lead to the data center floor are frequently an area where proper security measures are overlooked. It is helpful to think of the gray space as the perimeter to the data center and secure it appropriately.

### Who is in the Gray Space?

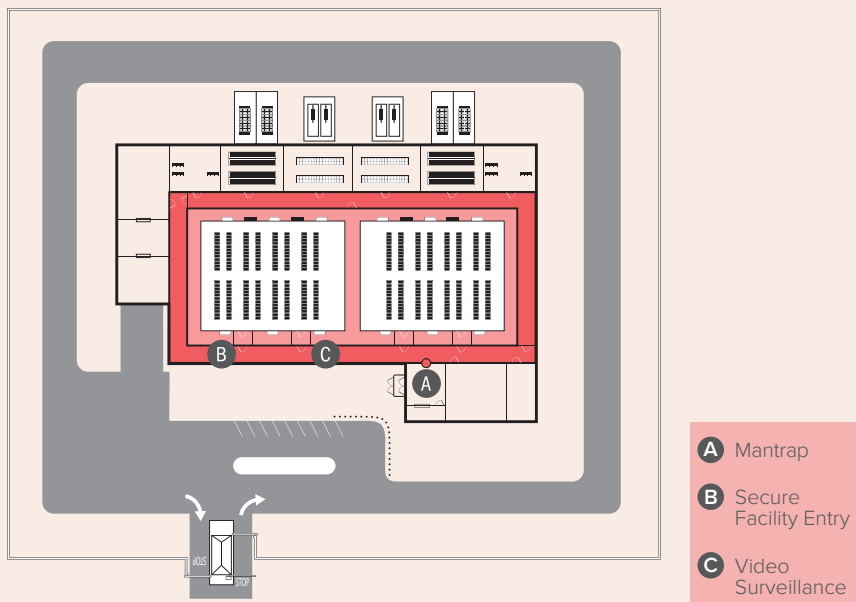
Visitor control is critical. Without proper visitor tracking if a group is touring a facility, it is not difficult for someone to slip away to use a restroom and not be noticed if they fail to return. There is now an unescorted, unaccounted for visitor one open door away from the data center white space.

### Mantrap In and/or Out

Allowing only a single person in is obviously more secure than allowing a group. Users of a mantrap, and truly all secure areas of a data center, must be aware of potential “tailgaters” who follow an authorized individual closely to bypass the proper security procedures. Even if the individual is authorized, tailgating is a breakdown in the ability to track those in the data center and must not be permitted. A strict policy should be in place that does not permit such unauthorized access.

A mantrap is frequently used either into the gray space from the reception area or out of the gray space into the data center halls. This is not mandatory, but it is helpful for higher security installations.

**Figure 14:** Layer 4: Hallways, Escorted Areas and Gray Space



## Building Infrastructure Access Control

Once in the gray space, it is much more attainable for someone to penetrate the power and telecommunication systems that provide the backbone of a data center, along with their backup systems. The security of a building's infrastructure is a paramount concern for any data center and multiple security methods should be in place to protect it. A mechanical key cylinder is not difficult for a motivated and skilled malicious individual to defeat. A catastrophic incident can occur if an unauthorized person accesses important building infrastructure from the gray space.

Every door in a facility that does not have active access control is a possible problem point. Many of these doors can be accessed via the gray space by someone who passes through the main security entrance of a data center if the gray space is not properly monitored.

## Secure Doors and Locks

Doors that lead from the gray space into infrastructure or other areas should be considered for high-security doors and lock sets. Locks that engage not just at the door handle, but at the top and hinge side provide a greater level of protection should an opening of the cylinder lock occur.

## Video

Video is an important tool in securing the gray space, and it can provide good, clear coverage of the hallways. A video strategy can include:

- › High-resolution cameras ranging from HD 720p and 1080p to multi megapixel
- › 360° degree or 180° degree cameras that can cover a significant area
- › Cameras with speakers and microphones to enhance the ability of security personnel to judge potential situations and converse with subjects
- › Motion detection that can alert to movement within sensitive areas or network cameras that come with intelligent motion detection that allows multiple specific points of interest to be masked off for motion detection versus the entire field of view
- › Identification of who went into the chiller plant or the battery room and confirm their access.

## Proper Emergency Plans

An additional area of concern is fire exits from all points of the facility. What happens if somebody pulls a fire alarm? Would a visitor suddenly have access to areas that would be off limits without the emergency? Would data center employees know what to do?

## LAYER 5: DATA CENTER ROOM AND WHITE SPACE

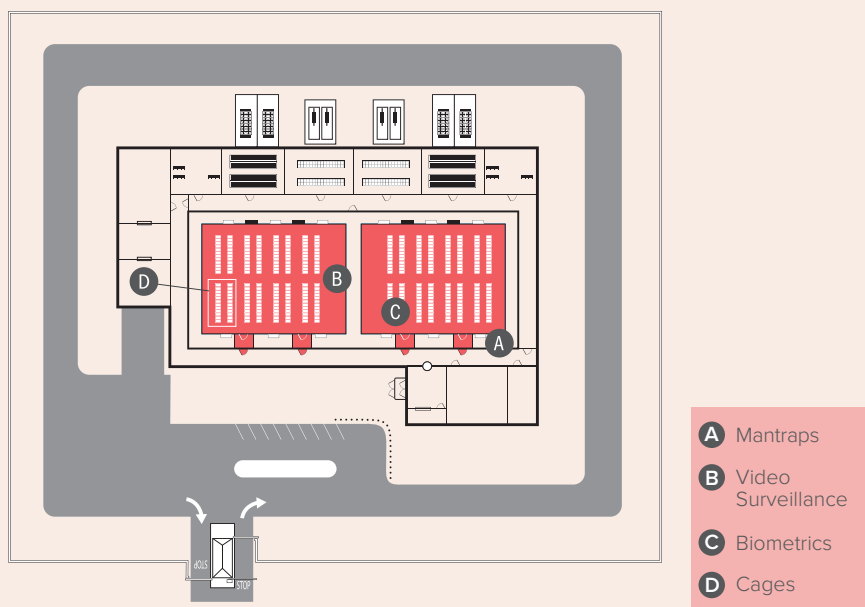
As the importance of each layer of protection is explored, it becomes obvious that each individual layer of protection is extremely important. A threat can do great damage once inside a data center cabinet, and it speaks to the importance of controlling access to the data center room and white space. Someone intent upon server theft or a virus upload cannot achieve that if access to the floor is not granted.

If there is an overall strength in data center security, it is likely the focus that is placed on preventing unauthorized people from entering the white space. Regardless of this focus, many data centers still have holes in their plans, processes or systems that render the white space not as secure as it could be.

### Mantraps

Part of the security feature in and out of many data center rooms is a mantrap. The mantrap requires authorized access into a small room, where both sides of the door must close and then another authorization procedure takes place to clear an individual for entry.

**Figure 15:** Layer 5: Data Center Room and White Space



## Cages

Within the white space, a cage system can provide enhanced protection to separate and secure customer specific cabinets or network equipment. When using a cage system you should ensure your desired security measures for access control, intrusion detection and video surveillance can be supported.

## Video

There are many uses of video throughout the different layers, but specific to the data center room and white space, there are specific cameras that can be used. A 360° degree can be used in the middle of hot or cold aisle. Based on how it integrates with the cabinet access control, it digitally zooms into a preset position when a cabinet door is opened.

A pan-tilt zoom camera can be used at the end of a row as a fixed-position camera. It is stationary and looks down the row in its home position. Once a cabinet is opened, it will automatically optically zoom in and record the person going into a cabinet based on a preset position, and then zoom back into its fixed home position.

Low-light cameras can also be used in areas where data center floor lights are dim when no motion is detected to save on energy costs. Advances in technology now allow these low-light cameras to provide color images in dark environments better than the human eye can see and provide more lifelike colors in low-light conditions.

Thermal cameras can be used in the data center to provide protection in the event a malicious individual intentionally turns out the lights in an equipment storage area or on the data center floor. Thermal cameras operate in complete darkness by providing a heat signature that always radiates from any object or person. Thermal cameras can also be used to find hotspots caused by overheating servers, uninterruptible power supplies, cooling systems and power distribution units inside data centers.

### VIDEO AS A BUSINESS SERVICE:

Cameras in the white space offer capabilities beyond just protecting people and assets. A high-resolution video camera can allow a user to visually identify equipment to see what's going wrong. This provides a forensics capability for reviewing what has taken place in the data center. Cameras can assist a network operations center by visually identifying and reading equipment displays and LED light patterns, allowing for more efficient monitoring and maintenance. Providing video surveillance as a business service is an added benefit of security video monitoring.

## Biometrics' Triple-Factor Advantage over Dual-Factor Authentication

Access control into the data center white space and between the white space and the data center cabinet is of primary importance. Some data centers, even those with otherwise high security protocols, still rely upon badges that require dual authentication even in protecting the inner core of a data center. Even though badges are still acceptable in the outer portions of the protective rings, best practices dictate the use of biometric identification closer to the data suite.

### What are the Three Key Advantages of Biometrics?

**Proof:** Biometrics, whether via fingerprint, iris scan or otherwise, positively proves an individual's identity. Keycards with dual authentication provides some semblance of security, but as anyone who has ever used a friend's or spouse's debit card can attest, possession of a card and knowledge of a PIN code is simply not proof of an individual's identity.

**Convenience:** Biometric systems avoid situations where a card has been lost or misplaced, which requires time, energy, effort and expense to deal with. A fingerprint or iris doesn't need replacing, making a more efficient and less time-consuming solution.

**Cost:** Even though a keycard reader is initially less expensive than a biometric reader system, the management costs of a system add up quickly. The initial issuance of such keycards can become costly, as is the replacement of misplaced keycards or those left at home.

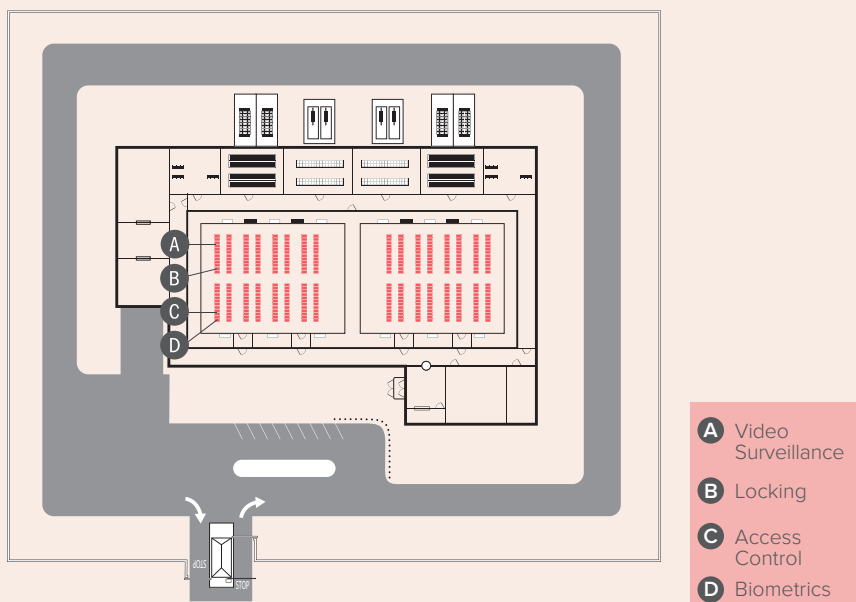
The cost advantage of biometrics is especially true in a facility that requires authorization for a large number of people to enter. The cost of biometric systems should not be a barrier for implementation; in the long run, it is frequently less expensive, as there are few costs beyond that of the reader. Even though a biometric reader is more expensive than a keycard reader, there are not the initial and ongoing costs of the keycards themselves, which typically cost around \$3 a piece. If over time the number of employees and visitors requiring keycards becomes a fairly large number, the keycard reader system will frequently be more expensive than the biometric system.

## LAYER 6: DATA CENTER CABINET

The core of the data center is the IT infrastructure housed within a data center cabinet. As a rule, these cabinets are remarkably insecure.

Cabinet access control is being implemented into more compliance standards. The ability to positively identify who is getting into those cabinets is now required for TIA Tier 3 or Tier 4 data centers, and PCI DSS is one of the many certifications that is continually raising the bar on standards. The vast majority of data centers lack proper cabinet access control. This is a significant issue.

**Figure 16:** Layer 6: Data Center Cabinet



## A Key Problem

A common problem is that many cabinets today are still being shipped with a single master key. Surprisingly, each override key can open all other cabinets of the same model in any data center anywhere. As a result, the majority of cabinets in use by data centers today can be opened by anyone who possesses one of the override keys.

This situation creates a significant gap in the security of many data centers, where somebody with a manufacturers' override key can quickly and easily access a cabinet. The implications of this ready access to a data center cabinet have significant consequences, including the following:

- › **Server theft:** Server theft is surprisingly common, and according to DCD the average price of a data center server in 2014 was \$7k but the disruption caused is far more
- › **Storage theft:** The average price of a storage system in 2014 was \$12k according to DCD – but the loss of data could be very significant
- › **Virus upload:** A similar concern is the ability to upload a virus when given access to the cabinet.
- › **Interruption with power or connectivity:** No matter how redundant a data center, if a server has wires clipped, there will be a period of downtime until the problem can be diagnosed or fixed.

This is obviously a significant issue for all data centers, but particularly in data centers with a lot of visitors and foot traffic through the facility. It should be a particular concern of multitenant data centers where a customer's representative (a technician or contractor) can be legitimately cleared to be inside one customer's cabinets in easy reach of other customers' cabinets. If they possess the proper manufacturer's override key, and are not properly monitored, they would have easy access to other customers' servers and infrastructure.

In many multitenant data centers, a customer's IT infrastructure can easily be accessed by the customer next door, but this isn't just a multitenant data center problem. Few data centers do not at least occasionally have outside contractors and others doing work on the data center floor. Whether it's a private data center or a co-location environment, a contractor or employee with malicious intent can quickly and easily access a data center cabinet and do significant and expensive damage in a very short period of time.

Co-location facilities also frequently have significant foot traffic with people on sales tours and many try to host events for technologists and other business leaders in an effort to increase awareness of the facilities. Those additional visitors create additional need for a cabinet access control solution.

## Key Restrictions

If circumstances dictate the use of a cylindrical key access, some steps can be taken to reduce the risk.

- › Understand that “do not duplicate” is meaningless in an era of self-serve key replication machines in major retailers.
- › Some manufacturers have key blanks that are stamped with end-user ID numbers, which enable the manufacturer to identify the source of any unauthorized keys.
- › Always be aware that a key system with no other cabinet access control is sub-optimal and is a significant security risk.

## Best Practice Support

Basic security best practices can mitigate the risk somewhat. Policies that can reduce the risk include strict tracking of all those given access to the white space, requiring escorts for visitors, not allowing individuals to be alone on the data center floor, and requiring two or more team members together whenever they are in the white space. While serving as deterrents, none of these methods is completely foolproof.

A plan for cabinet access control is also needed for private data centers as well. It is not rare for a data center to have instances where staffers have reason to be in the data center space regularly but not necessarily in the cabinets.

## Cabinet Access Control Products

In recent years, a number of access control products that attempt to solve the issue of cabinet-level security have come to market. Typically, these products use dual (or greater) factor authentication or biometrics in an effort to make sure that only those with proper clearance have access to a cabinet.

## An Audit Trail

Access control products must create complete access records to support a true level of security and compliance via a verifiable audit trail. They can also limit access to specific times for specific individuals. For example, a contractor that works on a server on Tuesday mornings can have access restricted to 8 a.m. to noon on Tuesdays.

## Interoperability and Video

Cabinet access control is improved by including video integrated for visual confirmation as well as access control. Integrating video surveillance and access control creates a verifiable audit trail of those who are within a cabinet. Many customers are insisting upon interoperability from manufactures and security integrators.

## End-of-Row or Integrated Cabinet Reader

Cabinet access can be controlled by either an integrated cabinet reader at the handle or by an access device at the end of a row. As a general rule, end-of-row solutions are more affordable but do not provide as detailed an audit trail on a cabinet-by-cabinet basis as an integrated cabinet reader provides. Every application will be unique. In addition to budgetary factors, the system size, future scalability, needs, security requirements and policy and procedures should all be factors in the decision.

## Key Override

In case of an emergency situation or power loss, a person in authority may have need for a key that bypasses all other security measures. The presence of a manual override key obviously requires significant management, including the following best practices:

1. The key system must be restricted by a utility patent to prevent unauthorized key duplication.
2. Override keys must be tightly managed to make sure they are only used by authorized users.
3. Keys should be locked in a safe or emergency key cabinet that has restricted access.
4. Keys should be logged in and out – and only by authorized users.
5. Cabinet access control system should be able to detect and log any use of bypass keys.
6. Keys should only be used in emergency/power loss situations.

## Proper Procedures and Cabinet Access Control are Keys

The risk of penetration to a data center cabinet is obvious, and the large numbers of manufacturer keys in circulation increases the risk. A combination of a solid plan, proper security procedures, a dedicated adherence to those procedures, and new tools and technologies are necessary to properly secure a cabinet.

# CONCLUSION

---

Creating a security strategy isn't a one-size-fits-all proposition. By using the "Defense in Depth" approach outlined in this report, data centers can create a secure environment by using multiple security strategies, policies and protocols. Whether it's a military-grade installation, a multitenant facility or even an on-site data center of a local business, the six layers help create a Defense in Depth posture, tailored to each individual's need, to protect critical infrastructure, deter potential threats and promote the achievement and maintenance of necessary compliance objectives.

Data breaches are becoming nearly universal, and data centers of all sizes need to be aware of the risks and prevention strategies. As more data are created in all areas of personal and professional life, the information stored in the cabinets becomes increasingly valuable. Evaluating and budgeting for logical and physical security is the only rational step.

Never before has a data center breach been more damaging to the future of an organization. As the risk has risen, a growing array of sophisticated threats continues to emerge designed to penetrate data center defenses. It's important to take the first steps now to develop, implement and execute a suitable data center physical security strategy.

Contact Anixter to learn about how risk management works with the other building blocks of Anixter's Infrastructure as a Platform solution. Infrastructure as a Platform focuses on helping you create an agile and scalable data center by addressing the five key building blocks for data center interoperability:

- > Risk management
- > Network migration
- > Power optimization
- > Thermal efficiency
- > DCIM enablement

For more information on how to secure your data center and reduce the risk of a data breach, visit [anixter.com/datacenterdcd](http://anixter.com/datacenterdcd) or contact your local Anixter representative.

SPONSORED BY ANIXTER'S TECHNOLOGY ALLIANCE PARTNERS





At Anixter, we enable the connected world. From securer facilities and communities, to more efficient networks and industrial environments, we deliver the infrastructure solutions—and intelligence—that sustain your business.

Through our unmatched global distribution network, supply chain management expertise and technical know-how, we drive efficiency and effectiveness to benefit your bottom line.



DatacenterDynamics (DCD), part of the DCD Group, is an international B2B media and publishing company. It offers a comprehensive range of products and services to assist senior professionals in the world's most ICT-dependent organizations in their risk-based infrastructure and capacity decisions.

DCD's portfolio of live events, online and print publishing, business intelligence and professional development brands are centered around the complexities of technological convergence. Accessible from over 42 countries, DCD's unique knowledge and networking platform is trusted by over 40,000 ICT, Engineering and Technology professionals worldwide.

**FOR MORE INFORMATION:**

**+44 (0)20 7426 4813**

**[info@dcd-intelligence.com](mailto:info@dcd-intelligence.com)**

**[www.dcd-intelligence.com](http://www.dcd-intelligence.com)**