# THE FOUR LAYERS OF DATA CENTER PHYSICAL SECURITY FOR A COMPREHENSIVE AND INTEGRATED APPROACH

ANIXTER

Products. Technology. Services. Delivered Globally.

## CONTENTS

## INTRODUCTION

One only has to look at a recent headline to grasp the increasing importance and urgency surrounding data center security: "Credit Card Data Breach Affects 1.5 Million Cards."[1] This recent breach of credit card numbers at Global Payments, a processing vendor for Visa, underscores the risks inherent with storing confidential and valuable data.

The ramifications of allowing a data breach can be devastating to companies of any size. Besides the loss of confidence by business partners or customers that may entrust their data to you, there is often a significant financial fallout. In the Global Payments case, they were dropped by Visa and estimates place the financial loss at more than $100 million.

Even though this is a worse-case scenario, the 2012 Cost of a Data Breach Survey, which includes 49 U.S. companies in 14 different industry sectors, showed some sobering results:

- The average cost of a breach is $5.5 million.
- Negligent insiders and malicious attacks are the main causes of data breaches.
- 39 percent of organizations say negligence was the root cause of data breaches.
- Malicious or criminal attacks account for 37 percent of total breaches.

Some industries in particular, such as financial and healthcare, are responsible for mass amounts of highly sensitive data, such as social security numbers, medical records and credit card accounts. Multitenant data centers must also be extremely vigilant in order to protect their customers' data.

There's no doubt that data breaches are here to stay, and the threat will only grow worse. Every CIO and IT manager will have to grapple with these challenges and make data center security a priority. In fact, as digital data continue to flood into data centers via cloud computing, tablets and smart phones, those charged with securing these valuable facilities must assess their risk, including the threat of physical breaches from outside and within.

## TECHNOLOGICAL AND INTERNAL CHALLENGES

Like many emerging technologies, those related to data center security often lack standardization, multimanufacturer interoperability and a unified communications infrastructure to exchange information across multiple subsystems. Even though this will change and improve over time, with much of the progress driven by industry standards and regulatory requirements, today's best security solutions focus on cost effectiveness, reliability and performance.

For example, IP-based physical security systems are now replacing legacy and closed-loop systems, which allow all services to converge and operate over a single protocol framework. In a new data center, it is recommended to plan your security system on an IP-based solution in order to benefit from current and future technologies being developed around the Ethernet standards, the de facto network protocol for private and public communications networks.

From an internal or corporate cultural perspective, another challenge can be the lack of security awareness and cooperation between security or facility personnel and IT staff. Even though IT and security personnel can differ widely on priorities and approach, it's important for both parties to work collaboratively toward the same goal: optimum security for the data center.

## INDUSTRY STANDARDS AND LEGAL REQUIREMENTS

When designing the physical security of a data center or improving upon existing facilities, there are several industry standards as well as legal requirements for organizations charged with safeguarding sensitive or confidential data. In some cases, there may even be fines levied for noncompliance, so it's vital to have a solid grasp of data center security requirements. Below is a brief overview of some applicable standards and legal requirements.

**SSAE 16:** Statement on Standards for Attestation Engagements (SSAE) No. 16 replaces the previous Statement on Auditing Standards (SAS) No. 70. The SSAE 16 is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). This standard demonstrates adequate controls and safeguards for host or process data belonging to customers. Some of these controls include physical security requirements such as two levels of authentication for electronic access, "man traps" on the data center floor and a provisioning process for individuals requesting access. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SSAE 16 even more important to the process of reporting on the effectiveness of internal control over financial reporting.

**ANSI/TIA-942:** The ANSI/TIA-942 data center infrastructure standard also provides information to planners regarding the protection of data center assets whether by means of physical security or fire prevention. Within its guidelines, it recognizes the importance of providing manageable access control to data center facilities and monitoring of people and their actions. Using the Uptime Institute Tier framework as a basis, the ANSI/TIA-942 standard makes recommendations on improving the physical security of the data center. These include criteria such as video surveillance recording frame rates, access control levels and hardware, and site selection.

**Sarbanes-Oxley, Other Legislation and Standards:** Sarbanes-Oxley, HIPAA (Health Information Security Rule Safeguard Standards) and PCI-DSS (Payment Card Industry Data Security Standard) not only mandate that certain access restrictions be in place for data center facilities, but also require the reporting and auditing of access be provided—potentially in real time. In addition, certain directives from the Department of Homeland Security may apply to your data center if the data you house is deemed vital to national and economic security.

As governmental regulations increase, advances in IP-based physical security are creating better, more simplified systems. Controlled access, reporting functions and accountability that IP security systems can deliver assist companies in meeting regulations and requirements.

## OPTIMUM PHYSICAL SECURITY: LAYERING IS THE KEY

There's no better example of the high priority leading companies place on physical security than a top-secret financial data center on the East Coast. The design of this 8-acre facility is a model of a serious approach to physical security with perimeter safeguards such as hydraulic bollards to stop speeding cars and a drainage pond that functions as a moat. This fortress-like design continues inside and—although some of the security safeguards are confidential—the command center reportedly features a 40- x 20-foot wall of screens that monitors an extensive network of high-definition video cameras, high-tech entry point technology and much more.

Although not every facility will require a moat or a NASA-like command center, the increased use of virtualized computing environments and hosted cloud computing services have only increased the critical need for data centers to provide 100 percent uptime and secure business operations. As the data in a data center become more valuable, protecting that asset becomes more critical. Sabotage, theft and uncontrolled access to a data center's assets pose the most immediate risks.

The most sound and strategic way to reach optimum physical security is to design and manage your data center in terms of layers. Layering creates depth in your physical protection structure, helping to confirm failure of one element in the system will not create vulnerability in the whole system. The inner layers also help prevent malicious or even unintended data breaches from employees.

**Security measures can be categorized into four layers:**

- Perimeter security
- Facility controls
- Computer room controls
- Cabinet controls

Addressing each of these layers provides comprehensive and integrated protection from the facility's perimeter to the cabinets in the data center.

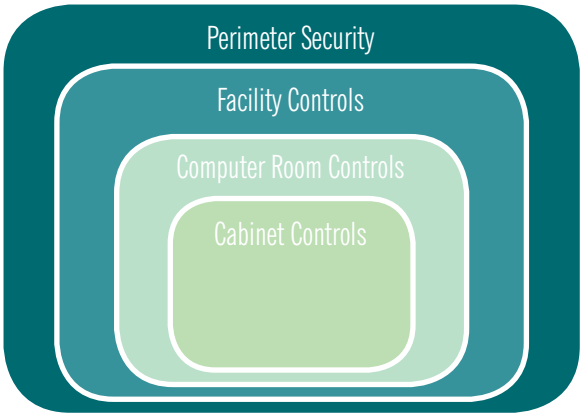


Figure 1: The Four Layers of Data Center Physical Security

## WHY INNER LAYERS ARE IMPORTANT

Even though the concept of physical security layering obviously makes unwanted entry originating from outside a data center facility more and more difficult, inner layers also help mitigate insider threats, which are often ignored. Consider the following survey's[2] results:

- 85 percent of employees admit to knowing that downloading corporate information from their employer is illegal
- 25 percent of employees say they would take the data anyway, regardless of penalties
- 41 percent of employees admit to having taken sensitive data with them to a new position
- 26 percent of employees say they would pass on company information if it proved useful in getting friend or family a job
- 72 percent of employers are moderately to extremely concerned that laid off or disgruntled employees will destroy company property
- More than 69 percent of employers see full-time employees as the biggest threat to security

Even though the insider threat can be the most elusive, physical security within the inner layers of the company, such as computer room and cabinet controls, can help secure the heart of your data. Various technology and security assets can be positioned to:

- Track people
- Limit unauthorized employee access to high-priority areas
- Provide an audit trail of personnel access
- Integrate with video to provide a record of an attempted breach.

In particular, the fourth layer of cabinet controls discussed below **(Figure 1)**, can be particularly effective in minimizing the insider threat.

## FIRST LAYER: PERIMETER SECURITY

The primary goals of the first layer of data center protection—perimeter security—are the three D's: deter, detect and delay.

As an example, a perimeter fence equipped with sensors can serve as the first detection point for intrusion. This perimeter fence detection system can be integrated with intrusion alarms, limited access control points, high-definition video surveillance and motion-activated security lighting. Security personnel will then be able to pinpoint an intrusion and immediately access the network's security system.

Besides site-hardening strategies, the perimeter video surveillance system can detect potential threats and intruders, too. For example, motion detection technology can trigger alarms, and video content analytics (VCA) can identify objects left behind, count people and employ other "smart" tactics to quickly spot real threats. The newest high-definition technology can help acheive the highest resolution, and edge-based internal camera memory storage can limit gaps in your perimeter. From a video resolution point of view, the trend toward HDTV surveillance cameras is transitioning from early to broad scale adoption in many commercial building applications. The benefits of HDTV cameras include using standard color and resolution profiles established by the Society of Motion Picture and Television Engineers (SMPTE) and using a 16:9 aspect ratio versus the 4:3 aspect ratio **(Figure 2)** used by analog cameras. These technological advancements make the video surveillance system more responsive to potential security breaches because activity in the perimeter layer can be quickly assessed.


Figure 2 : 16:9 ratio vs. 4:3 ratio
Image courtesy of Axis Communications

## OVERCOMING PERIMETER RESTRICTIONS

In some cases, the environment, the existing infrastructure or the budget may restrict physical security at the perimeter layer. If so, it may not be possible to install heavy-duty fencing, gates and barriers at your data center facility. Installing alternative or complementary solutions, which include sensors (sensitive fiber-optic cable, passive infrared (PIR), etc.), VCA, and network camera-based technologies, enhance even the most basic physical barriers or can create virtual barriers around a site.

## SECOND LAYER: FACILITY CONTROLS

The goals of this secondary layer of protection are to further restrict access if a breach has occurred at the perimeter. Indoor surveillance for identification and monitoring, as well as multiple ID verification methods are a must.

By using visitor management and high-resolution video surveillance systems, facility controls measure, monitor, and restrict access to the building. The type of facility—a dedicated private facility, a multitenant or co-location facility, or a multifunction enterprise facility—will determine the appropriate levels of security controls needed to balance between needed security and visitor experience. For example, it may not be suitable for CEOs and customers to pass through "man traps" at a corporate headquarters, so a less intrusive system may be required.

Another technological advancement that is facilitating the use of high-resolution video is H.264 Advance Video Coding (AVC). Bandwidth allocation and preservation is a principle concern for many IT managers and as video surveillance migrates onto the corporate network, steps must be taken to confirm that bandwidth usage as well as the video storage requirements are minimized. H.264 AVC can reduce the bandwidth consumption associated with high resolution video streaming by up to 80 percent when compared with traditional coding methods such as Motion JPEG **(Table 1)**.

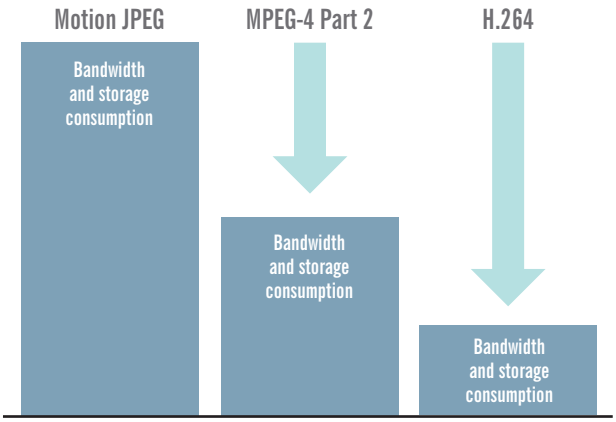


Table 1: H.264 Bandwidth and Storage Consumption Comparison

Consideration should also be given to the cabling infrastructure as well. IP-based video is delivered through the network in real-time, typically using User Datagram Protocol (UDP), which is the transmission of data from one node on the network to another, is not guaranteed. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system such as video.[3] Therefore, it's critical that the physical layer systems, such as the cabling infrastructure, not cause transmission errors on the network. Simulations of worst-case cabling and network equipment conditions conducted in the Anixter Infrastructure Solutions Lab demonstrate the benefits of using higher bandwidth cabling systems when the installed network environment is less than ideal **(Figure 3)**.

**IP Video**-Minimally Compliant Category 5e

**IP Video**-Category 6

Figure 3: Comparison of IP Video on Minimally Compliant Category 5e and Category 6 Cabling

Integrating access control and instruction systems with video surveillance via an IP network can verify and enhance performance. For example, video surveillance can verify the identity of a person entering an unmanned access control point by capturing video as the person swipes his access card. It can also account for instances of "tailgating" or "piggybacking." Video Content Analysis can be used to count the number of people going through a doorway, for example.

More complex video analytics can read license plates, conduct facial recognition and detect smoke and fire threats. An integrated system can rapidly verify tripped alarms such as fire alarms from a safe location, which allows for a speedier response in the event of a fire.

The continuation of an open-architecture video surveillance system deployed on an IP network allows security personnel to observe visitors as they make their way from a parking garage or outside a building to the reception, then further track them throughout the data center facility. Again, video surveillance can be integrated with new visitor management technology to help people keep to their specified areas of access.

## THIRD LAYER: COMPUTER ROOM CONTROLS

The goals of the third layer of physical security are to further restrict access through multiple forms of verification, monitor all authorized access, and have redundant power and communications.

Access to the data center computer room or "white space" is restricted to a set number of individuals. To a certain degree, the measures in place will be the same from site to site. Deploying entry restrictions such as turnstiles, Video Content Analysis, biometric access control devices, radio-frequency identification (RFIDs) and environmental monitoring can help to restrict access by multiple verifications.

There are three basic methods for verifying someone's identity:

- Possessing or carrying the correct key or token
- Knowing predetermined private information, such as a password or personal identification number (PIN)
- Providing information that is inherent and unique to that individual, including the use of biometric devices to verify finger and thumb prints, irises or vascular patterns.

According to the Chemical Facility Anti-Terrorism (CFAT) performance standards for a Tier 1 facility, the identity verification system should be "vigorous," and "all unescorted personnel are issued electronic photo ID badges that are integrated with the facility's access control system" (RBPS Metric 3.2). Additionally, the SSAE16 auditing requirements state that access to all entry points into and within the data center should be protected by electronic access control mechanisms that allow only authorized individuals to enter the facility. Included within the framework of electronic access control should also be biometric safeguards, such as palm readers, iris recognition and fingerprint readers.

## FOURTH LAYER: CABINET CONTROLS

The fourth layer of data center physical security further restrict access and continue to work within an integrated systems framework. Security measures to achieve this include cabinet-locking mechanisms, audit trails and an intelligent infrastructure strategy.

The fourth layer is particularly important and effective in minimizing the significant and often-ignored "insider threat" discussed earlier. Many data centers do a good job at executing the first three layers, but the absence of reliable cabinet controls can result in a costly data breach caused by a disgruntled or malicious employee, or perhaps even innocent and unintended data access.

Assuming all previous layers of security are implemented, access to server cabinets and storage, and the invaluable data contained in them, should be restricted to authorized personnel. However, in a multitenant or private facility, the potential for accessing, compromising or destroying data—intentional or not—needs to be reduced, monitored and audited.

Some key considerations for that critical fourth layer:

- Reliable electronic locking systems for server cabinets are recommended.
- Integrated solutions that use similar security techniques as accessing the room—even the same access cards and biometrics—offer intelligently managed access to cabinets.
- By further restricting access, these systems can be linked with networked video to capture images or clips of the person at the cabinet and their activities, automatically creating logs for audit capabilities.
- Integrating access control and video surveillance on an IP network enables you to deploy further steps, such as presetting pan tilt zoom cameras to go to different positions based on cabinet doors opened.

There is a wide range of locking hardware from simple mechanical locks to fully intelligent locking hardware that can be considered for cabinet and caged environments **(Figure 4)**.


Figure 4: Types of Locking Hardware

## THE SECURE DATA CENTER

Technological advancements in cable and electronic devices, such as network cameras, video management and recording platforms, and intelligent access control hardware and software have enhanced the possibility of a totally secure data center. Applications that take advantage of IP networks have provided an integration platform for the four layers of security to create an effective, efficient and comprehensive system.

By creating more efficient image and data management through the migration of security to the IT realm, the IP network allows for better recording, storing, searching, retrieving, sharing and sending capabilities. This results in a more structured and standardized approach, as well as shared responsibilities across IT and security teams.

However, it's worth noting that a comprehensive IP system doesn't have to be deployed from scratch. With the right expertise, companies can leverage many existing physical security assets and bring their overall data center security closer to best practices and industry standards.

It's vital to address all four layers, in particular, that often forgotten fourth layer that helps mitigate the insider threat. By focusing on all four layers of physical data center security, your team will embrace a comprehensive approach that ensures all threats—whether from outside or within—are addressed, minimized or completely eliminated.

**For more advice and information on planning and deploying a comprehensive security system to protect a data center, please contact your local Anixter representative.**

## REFERENCES


[1] Jessica Silver-Greenberg, New York Times, Business Day, After a Data Breach, Visa Removes a Service Provider, 1 April 2012

[2] Cyber-Ark survey of 600 financial industry workers in New York and London via InformationWeek and Actimize surveys

[3] Kurose, J. F.; Ross, K. W. (2010). Computer Networking: A Top-Down Approach (5th ed.). Boston, MA: Pearson Education. ISBN 978-0-13-136548-3.

**Electrical and Electronic Wire & Cable • Enterprise Cabling & Security Solutions • Fasteners**

Anixter Inc. World Headquarters • 2301 Patriot Boulevard, Glenview, IL 60026-8020 • 1.800.ANIXTER • 224.521.8000 • anixter.com

Anixter is a leading global supplier of communications and security products, electrical and electronic wire and cable, fasteners and other small components. We help our customers specify solutions and make informed purchasing decisions around technology, applications and relevant standards. Throughout the world, we provide innovative supply chain management solutions to reduce our customers' total cost of production and implementation. A NYSE-listed company, Anixter, with its subsidiaries, serves companies in more than 50 countries around the world. Anixter's total revenue approximated $6.1 billion in 2011.



12F0010X0 © 2012 Anixter Inc. • 10/12