Biometric Physical Access Control in Data Centres: Ensuring Regulatory Compliance, with Indisputable Audit Trails

Adapted by Andy Billingham, Managing Director – EMKA (UK) Ltd
from an original report by Digitus Biometrics

Overview

Maintaining compliance with various data privacy rules and regulations – PCI DSS, HIPAA, FISMA, and more – is often seen as primarily a matter of securing data networks against unauthorised access. However, data privacy directives invariably focus on physical security as well as network security, and consider the protection of physical assets to be as important as protecting the data stored or processed in those assets.

Physically securing private information in data centre's has proven challenging, however, as the necessary technology has lagged far behind network security technology. The network security industry is a steady stream of innovative response to high-tech threats. For most data centres, physical security rests with technology from the last millennium.

This white paper explores an advanced security methodology by which enterprises can best secure physical assets within their data centres, with greatly enhanced security against the growing trend of insider threats and a 100% indisputable audit trail of physical access. The result is a more thoroughly secured operation that follows best practices for asset protection, reduces the risk of physical security breaches, and demonstrates the highest effort for regulatory compliance.

Biometric security at a data centre

Commonality among Data Privacy Directives

When boiled down to their essence, data privacy rules and regulations all seek to accomplish the same thing. Government regulations and non-government standards invariably ask four basic questions regarding access to sensitive information:

- Do you have safeguards in place to control access to sensitive data?
- Are you able to continuously monitor who is accessing sensitive data?
- Are you alerted in real-time when information is being accessed without authorization?
- Can you produce an audit trail showing who has accessed sensitive data and when they accessed it?

It's important to remember that "access" within the context of these questions means physical access as well as network access, and that specific requirements for controlling physical access exist in all rules and regulations concerning the protection of private or sensitive information.

Following are examples that span multiple industries:

• PCI DSS Requirements 9 and 9.1: “Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.”

• HIPAA Title II, Physical Safeguards: “Access to equipment containing health information should be carefully controlled and monitored. Access to hardware and software must be limited to properly authorised individuals.”

• FISMA (FIPS 200 Section 3): “Organizations must limit physical access to information systems, equipment, and the respective operating environments to authorised individuals.”

These regulations also share a commonality in the requirement for alerts and audit logs of physical access opportunities, though all are notably lacking in specifics regarding implementation. In each regulation, a covered entity must consider its risks and determine for itself reasonable and appropriate physical access alerting and auditing methods for information systems that contain or process the data being protected.

In practice, even those enterprises that are highly concerned about addressing risks related to physical access have been unable to elevate alerts and audits to the level they can for network security. This is primarily a matter of deficient technology, as 100% accurate alerting and auditing solutions for physical access have typically extended no further than a data centre’s front door.

Shortcomings in Common Physical Security Practice
Data centres are usually physically secured with a mixture of unconnected platforms that may include palm readers, proximity card readers, and keyed locks.

Because of their size, palm readers, the most secure platform in this group, are found only on doors. Servers that handle especially sensitive data are typically protected from data and device theft by locking server cabinets that are accessed with keys or key cards. The use of mixed access-control devices can raise serious issues as regards both sound security practice and the ability to demonstrate regulatory compliance.

The problem begins with the fact that keys and key cards can become separated from their authorised users. Any key or key card that is forgotten, lost, stolen, or otherwise separated from an authorised user represents a potential, undetected security breach. The greater the number of keys and key cards in a given environment, the greater the possibility of unauthorised access to physical assets in a server cabinet.

As a result, there is no effective means to issue an alert when unauthorised access occurs, and audit trails are incomplete. When an unauthorised user opens a cabinet with a working key card, there is a log entry but no alert. The audit log from a palm reader at a data centre’s front door provides solid evidence of who was in the data centre at any given time, but beyond that, all that’s known is which key cards, and not which users, opened which server cabinets. If the server cabinets are secured with keys – or are not locked – there is no audit trail at the server cabinet level at all.

Technology to Eliminate these Shortcomings
In addition to providing extremely accurate identification for access control, db ServerRack offers several key advantages relative to the rack itself and, when paired with db Nexus, to the task of securing the entire data centre:

• Simplified security administration. With biometric access control, administration is greatly simplified compared to the mixed-solution environment found in most data centres. There are no keys or key cards to assign, track, retrieve, and reassign. Removing all access privileges is a matter of a few keystrokes within the Digitus Access Software, as is reassigning access to specific areas facility wide, or even among multiple geographies.

• Reduced opportunities for breaches. Because biometrics eliminates the user of access enablers that can become separated from their authorised users, there are far fewer opportunities for security breaches. The authorised user absolutely must be present for access to be granted at any biometrically controlled checkpoint.

• Indisputable audit trail. Especially of interest in demonstrating compliance with government regulations concerning data storage, biometric access control produces an indisputable audit trail. db ServerRack extends that indisputable audit trail to the server cabinet. When paired with db Nexus, that audit trail can cover the entire enterprise, recording and reporting each instance of each individual's access from door to door to cabinet, and the exact time of each access – indisputably.

Although no data privacy rule or regulation specifies biometrics as the specific means to secure physical access, the Digitus solution unquestionably provides the most secure methodology available for addressing the intention of those rules and regulations, and its implementation is sure to satisfy even the most thorough regulatory audit.

Biometric swinghandle with fingerprint sensor and emergency opening

Scanning fingers on a touch screen

Conclusion: Ensure Regulatory Compliance for Physical Access across your entire Data Centre

The need to protect sensitive data has never been higher, from the perspective of both good business practice and regulatory compliance – and that applies to physical as well as to network access. Physical security does not guarantee compliance, and compliance does not guarantee physical security. But the availability of a single, networked platform that can deliver biometric access control to every access point within an enterprise, with an indisputable audit trail, is a strong step toward unifying compliance and security programs – from the front door to the server cabinets.

www.emka.co.uk
www.emkablog.co.uk
Patricia House
Bodmin Road
Coventry, CV2 5DG
United Kingdom
Tel: 024 7661 6505