How to protect micro data centres and individual defined high risk cabinets in data centres or co-location situations

By Andrew Billingham, Managing Director – EMKA (UK) Ltd

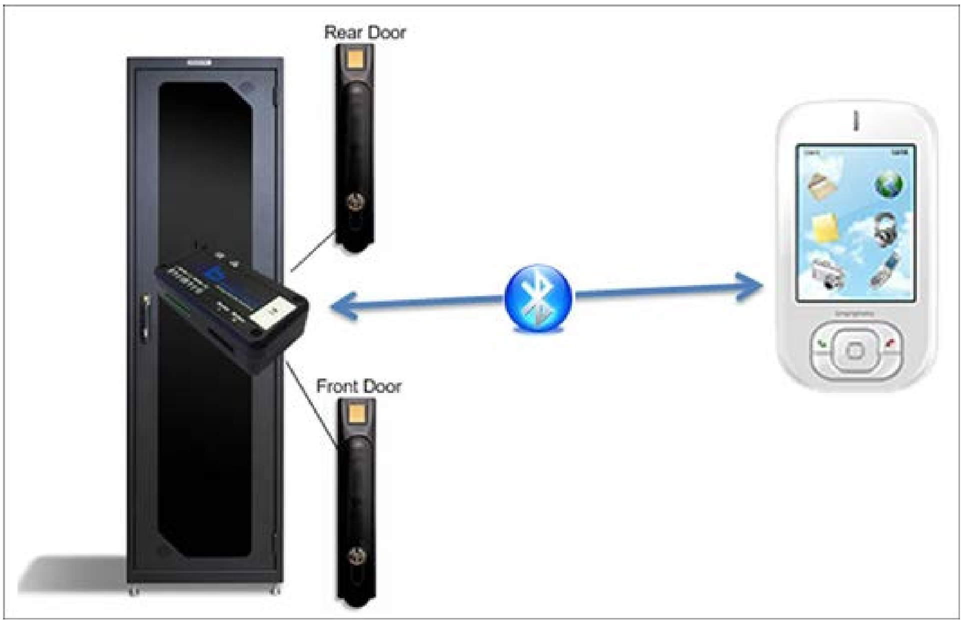
"How secure is secure?" According to the most recent studies, only about 20 percent of data centres are secure, leaving an overwhelming 80 percent at risk. It is likely that small centres are at the high end of this range. Fortunately there is wide commonality among Data Privacy Directives in that when 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.

In most centres 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, while 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.

Consequently it becomes important to review alternatives and although no data privacy rule or regulation specifies biometrics as the specific means to secure physical access, the EMKA/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. When combined with cards and PIN codes this 3 level system is truly at the forefront of security management in an unprecedented package.



The standing myth is that most threats of physical attacks come from outside the data centre; however, according to the Gabriel Consulting Group 2011 Data Centre Security Survey more than 60 percent of all malicious attacks on the data centre are by insiders. The people who are physical security threats, especially these insiders, have access to authorised cards, and sometimes other people’s cards. Additionally an authorised person can misplace their card or have it stolen. In fact the Global State of Information Security Survey 2013 by PwC, CIO Magazine, and CSO magazine found that 42 percent say their organization has “an effective strategy in place and is proactive in executing the plan.” However, on closer analysis, the same study found that only 8 percent of those respondents rank as truly secure.

It is to address exactly this large number of vulnerable standalone cabinets that the EMKA/Digitus Cabinet Sentry security locking system has been developed, using BioLock technology, to provide an extremely effective and efficient way of securing access to server cabinets using biometrics, iClass cards or proximity cards. The big advantage to Data Centre managers is the way that Cabinet Sentry brings biometric security to stand-alone data and control cabinets, also including vending machines, single cabinet data systems, vulnerable industrial controls, and especially for niche cabinets within larger establishments.

Cabinet Sentry can be used as a part of a networked system, or as a standalone product and is deliberately priced as a low cost solution since EMKA/Digitus believe that Data Centre Security is too important to be expensive.
This simple device of only 256 components in a compact 101.42mm x 51.46mm x 29.00mm package secures both front and back cabinet doors, offering a wide range of lock options working with EMKA based locks in networked or stand-alone configurations.

The EMKA/Digitus Cabinet Sentry is specifically designed for single cabinet use to secure both front and rear doors with biometric, proximity card and digital pin technologies as required. It is capable of managing up to 4 environmental sensors, e.g. temperature, humidity, air-flow, air pressure or water, and up to 4 variable sensor power outputs with either mains power + LAN or power over Ethernet (POE) connection. The Cabinet Sentry additionally features up to 2 auxiliary serial (RS232) inputs and may be integrated with 3rd party access control systems using its Wiegand output or via DAS-SQL so enabling 4G Bluetooth control by the Digitus dedicated mobile phone app.

Major Data Centre operators have long understood the need for physical access control on server cabinets, likewise in corporate facilities, where data stores are potentially exposed to a significant number of mission-critical employees, it is recognised that servers must be protected from thumb drive data theft and from theft of a server itself. Those same considerations apply to colocation facilities, which must also reassure customers that their servers are individually secure within a generally secured facility. Yet these server cabinets are rarely protected with the same level of security as facility doors. The most common method of physical access control at the server is to enclose it within a cage or cabinet featuring a mechanical keyed lock. Less common are enclosures that feature proximity readers. Both create significant risks.

As we have established, keys and key cards can be forgotten, lost, or stolen, and any key or key card separated from an authorised user represents a potential, undetected security breach. The only thing that’s known for sure in cabinet access is that an authorised person’s key or key card, but not necessarily the authorised person, opened the cabinet and of course this is where Cabinet Sentry is of value.

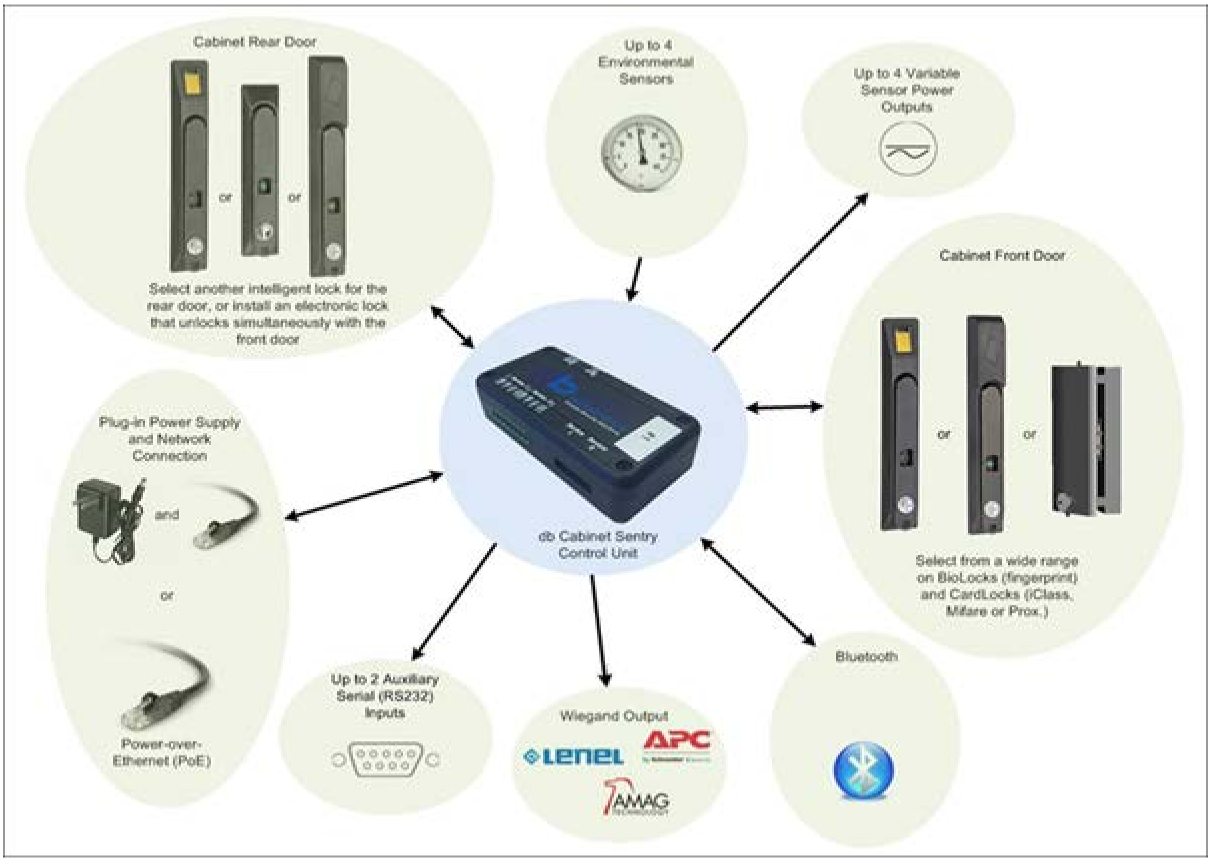
In addition while proximity readers offer an advantage over mechanical keyed locks in that they can produce audit trails, those audit trails are not indisputable. Again, they show only which card opened the lock – but not whose hand held it. Cabinet Sentry bio-security technology defines that the actual individual was present.

The benefits of this biometric security include:-

• 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.

• Reduced opportunities for breaches. Because biometrics eliminate the use 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 – which is especially of interest in demonstrating compliance with government regulations concerning data storage, biometric access control produces an indisputable audit trail.


Cabinet Rear Door
or
or
Select another intelligent lock for the rear door, or install an electronic lock that unlocks simultaneously with the front door
Up to 4 Environmental Sensors
Up to 4 Variable Sensor Power Outputs
Cabinet Front Door
or
or
Select from a wide range on BioLocks (fingerprint) and CardLocks (iClass, Mifare or Prox.)
Plug-in Power Supply and Network Connection
and
or
Power-over-Ethernet (PoE)
db Cabinet Sentry Control Unit
Up to 2 Auxiliary Serial (RS232) Inputs
Wiegand Output
Lenel
APC
AMAG
Bluetooth

We are all aware that 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. Although it must be recognised that physical security does not guarantee compliance, and of course compliance does not guarantee physical security, nonetheless the EMKA/Digitus approach offers peace of mind in that the traditional multi-layered perimeter approach has focused predominantly on the outside levels of perimeter defence:

- Keeping out “undesirables”
- Maintaining a clear zone between the outer perimeter and the reception area
- Gatekeeping at reception

- Service corridor security features
- Data room entry

Consequently the cabinets themselves have until recently been somewhat less regarded, as it is usually thought that low cost purely mechanical lock systems are perfectly adequate – if even this perimeter strategy was employed it is in any case an approach that is clearly insufficient for complete peace of mind.

With the increased level of cabinet security now offered with their Cabinet Sentry, EMKA take the view, with their technology partner Digitus Biometrics, that the security level should become more capable as an individual approaches physically nearer the core data store – rather than assuming a lesser requirement.

EMKA
(UK) LTD

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