Why Take Security All the Way to the Cabinet Door?

by Andy Billingham
Managing Director – EMKA (UK) Ltd

"How secure is secure?" This is the million dollar question … or literally, the 7.2 million dollar question - currently considered the average cost for a data security breach.

New 3500 program biometric locking system from EMKA offers greater personnel and data protection

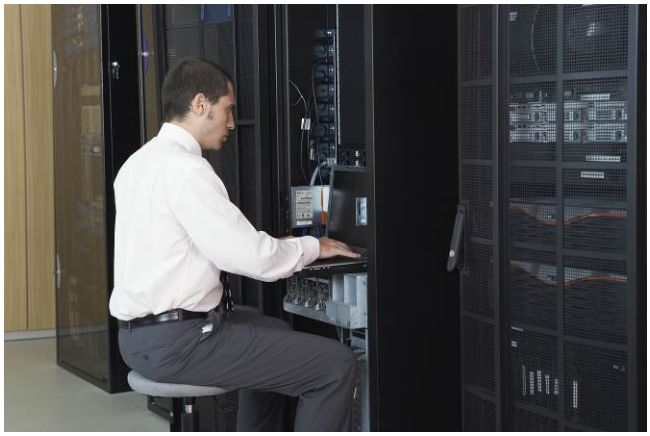
"How secure is secure?" According to the most recent studies, only about 20 percent of data centres are secure, leaving an overwhelming 80 percent at risk.

Security breaches aren't always as expected. A high priority is given to the outside threats of hacking into systems to steal information, but physical security proves to be one of the highest risk areas a company faces.

A perfect example of this happened to Switzerland's Intelligence Service when it was revealed that an employee who had been with the Service for 8 years was able to download anti-terrorist information onto thumb drives and walk out of the building with them in his backpack.

With that in mind, here are 3 reasons companies must take their security all the way to the cabinet door.

1. Most malicious attacks on the data centre are by insiders



Real time cabinet security software from EMKA UK for Electronic Locking and Monitoring System

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 concludes that more than 60 percent of all malicious attacks on the data centre are by insiders. The Swiss Federal Intelligence Service is a perfect example of this type of risk.

2. Current perimeter based security schemes do not provide adequate protection from threats

The traditional thinking, when talking about physical data centre security, is based on a militaristic perimeter access control methodology. The idea is to control access at the perimeter and then replicate the access control in reduced concentric circles. The idea is to slow the attacker as they try to make their way into the data centre and apprehend them prior to any damage being done.

While this appears strategically sound, there is one glaring loophole. The people who are physical security threats, especially the insiders, have access to authorised cards, and sometimes not their own cards. Additionally an authorised person can misplace their card or have it stolen.

3. Companies have an inflated false sense of security by underestimating the threat

Management often believes existing security schemes and systems reduce the vulnerability of the data centre to an acceptable level. Because there is simply a security strategy in place, management often have a false sense of security thinking it is “enough”

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.

EMKA BioLock – biometric technology at the handle for server security

Management’s assessment of vulnerability is often skewed and the resultant risk assessment becomes flawed. In most instances, this is fed by a cost avoidance mentality. This issue also points to poor communications between IT staff and management.

Under these scenarios, data centres are more vulnerable. Companies are learning that under the right circumstances it is no longer a question of “if”… but a question of “when.” Companies are finding that to truly protect their servers, physical security must play a top priority.

EMKA BioLock cabinet security is able to protect at this level.

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