Toward Zero Security Breaches with EMKA/Digitus Biometric Technology: 5 considerations for securing your sensitive data

by Andy Billingham, Managing Director – EMKA (UK) Ltd
- adapted from an article by Digitus Biometrics

If you manage your own data centre, colocation facility or technical data repository, then you know how important security is. It is essential that you safeguard sensitive information from physical theft, hacking, data breaches and human error. Fortunately, much has already been written about this topic, but this article is intended help you strengthen your security strategy going forward. Accordingly, we have identified 5 considerations that will help you protect your data centre:

1. Identify your physical weak points and determine your need
The first thing you need to do is figure out is where your vulnerabilities are. For example it is never a good idea to build a data centre against outside walls, similarly pay attention to what is housed above and below your data storage facility. By securing these weak points, you can eliminate the most obvious threat – someone breaking in. Small data centres especially may be located in a multi-floor building, in which case consider installing physical barriers, cameras and access control systems. Additionally, it is important to examine your operational processes so that visitors and contractors are not let inside your server room accidentally.

2. Keep track of all your workflow processes
It is critical that you keep track of your operations and compliance-related activities. You want to limit access to your data storage centre to IT staff and organizational stakeholders. As such, you should regularly monitor your access logs and perform audit checks. Keep track of peripherals, servers and data centre management software, looking for any suspicious activity. If your data centre is in a colocation facility, and you have a trusted provider, most likely your assets are safe and well-maintained. However, a prudent strategy should involve regular audits, regardless of where the centre is housed. Remember holding and managing data may well be the very core purpose of your organisation.

3. Watch out for human error
The most common form of data breach is that committed by insiders. It is now recognised that danger comes in the form of poor engineering, carelessness, or corporate espionage, but in all cases, people working in your facility pose the biggest risk. Accordingly, it is necessary that you implement strong security policies that hold personnel accountable for their access permissions. It is advisable that you pair access cards with biometric security, such as fingerprint scans, for the best possible defence. Biometric security is safer than passwords and much harder to replicate or steal. Employees will be deterred from lending each other access cards, and if one is stolen, it will be useless to the individual who tries to access your server room. It is important to understand that access should never be shared in an organisation.

Upon enrolment, the EMKA/Digitus Biometrics fingerprint reader creates a multi-point schematic of the user’s biometric fingerprint profile, which it stores as a 384-byte fingerprint template. This template will be matched to the user’s live fingerprint each time that user seeks to gain access. At no time is a fingerprint stored in the system. The system only retains the pattern recognition used by its algorithm.

If the fingerprint data perfectly matches the stored fingerprint template, the reader unit sends an encrypted “open door” command to the control unit. The unit then opens the electric lock and logs the date/time of the user entry.

Due to the precision of proprietary fingerprint recognition technology, fake fingers, the wrong finger, or a finger of someone deceased cannot fool the system and open doors to access secured areas. Further the authorized person may place on the reader a “duress finger” programmed into the system to send an alert to security personnel.

4. Educate your people on security policies
A big part of having a strong security system is staff member training eg explaining to staff why they should not lend each other access cards and instructing them to report any suspicious activity. Additionally, let them understand that for compliance purposes, workflow processes are strictly segregated and monitored. Often, regulatory agencies will want to see who access which piece of information and when. Eliminating duplication of access means that you are able to adhere to compliance standards with greater ease.

5. Ask your business stakeholders for their feedback
Once you have a security system fully in place, the next thing for you to do is discuss your policies with staff members. Ask them if they agree your assets are secure. Are they accessing data with ease? What are some potential vulnerabilities? It is also a good idea to talk to your IT staff and get their opinion on the matter.

Ultimately, as data becomes more central to business, enterprises will look for better ways to secure data. Biometric access control systems and two or three level extensions of these allow companies that manage data storage centres, colocation facilities, server rooms and the like to maintain better control of perimeter doors, interior rooms, cages and server racks – with one integrated platform. These sophisticated solutions help organizations prevent data breaches, hacking and problems related to human error. Additionally, these solutions reduce costs and simplify the authentication process for entry to secured locations.

Biometric locking system from EMKA offers greater personnel and data protection

EMKA BioLock – Biometric technology at the handle for server security

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