How can Access Control Systems Improve Security and Reduce Costs?

A Discussion Paper

Author: Nojmol Islam, Product Manager, ASSA ABLOY Security Solutions
Introduction

Building owners or facilities managers want a security solution that is convenient and cost-effective. In a difficult economic climate where capex is often restricted and with many businesses still operating on low margins, this is particularly pertinent.

At a time when the legal consequences and reputational issues arising from any failure to protect and secure people, physical assets and information data are increasingly severe, risks simply cannot be afforded.

The plethora of access control systems now available can address these issues by helping business owners find an adequate balance between security, risk and cost.

The question therefore is simple: how can access control systems both improve security and reduce costs?

The answers are complex and challenging but the issue is one of real importance. By producing this discussion paper, ASSA ABLOY Security Solutions wishes to stimulate debate and encourage views and contributions from many voices.

To contribute your opinion, experience or comment, please visit: www.facebook.com/ASSAABLOYUK or www.linkedin.com/company/assa-abloy-uk
Access control, at its most basic level, is a system that can either enable or prevent people from entering or exiting a location. This can be applied to a single room, or across a whole site.

A secondary function of access control may be to record the movements of building users in and out of locations. The data trails provided can be used for audit, traceability, improvement or compliance purposes.

The majority of access control systems rely on the person or asset transiting in or out of a location being recognised and validated. This is normally achieved through the use of a “credential.”

A credential can be broken down into three categories:

- **Something the person has:**
  - Key
  - Card
  - Identification Tag
  - Smartphone App

- **Something the person knows:**
  - Password
  - PIN

- **Something intrinsic to the person:**
  - Biometric data, such as:
    - Fingerprints
    - Iris recognition

In some systems, multiple layers of credential may be required. This is dependent on the requirements of the system, as identified in the specification process.

Some systems may require a second-party credential. This can include a second keyholder, or recognition by an approved inspector via a CCTV link.

As the number of layers and sub-systems increase, so does the complexity of integrating the system, and storing, accessing and making use of the data.

Despite the flexible nature of access control systems, the objectives are often the same:

- To protect building users from unauthorised access, which may threaten their personal safety or their possessions.

- To ensure building owners meet their statutory duty of care and other legal responsibilities, including health and safety compliance.

- To ensure the security of a building is versatile enough to efficiently manage the requirements of different users with varying levels of access.
What are the different types of Access Control?

**Standalone**
If a building needs to have a single room or door converted to an access control solution from a mechanical one, standalone systems represent a cost-effective method of implementation.

These are generally wire-free systems that can be applied to a range of construction materials, including glass, metal, timber or composite. These systems have a number of benefits:

- **Scalable**
  Standalone access control systems tend to be modular, making them fully scalable. This allows building development and future expansions to be achieved with ease.

- **Flexible**
  They can be tailored to suit specific security needs, in line with budget availability.

- **Environmentally Friendly**
  These units are often battery powered. By consuming low levels of energy, standalone systems can play an important role in helping a company achieve its carbon footprint goals.

- **Easy Implementation**
  Standalone systems can often be installed within a matter of minutes. There is minimal disruption to the day-to-day working environment, with pedestrian access rarely affected.

**Online or Offline Solutions**
Online access control means that the decision to grant access can be made by the Electronic Access Control (EAC) system.

Offline access control means that the decision to grant access is made by the device-based information stored on an asset or user credential.

These can be often be built in to standalone, or fully integrated systems.

**Fully Integrated | Wireless**
These types of access control systems can integrate fully with a building’s existing security solutions. Mechanical locks can be wirelessly integrated into existing access control systems with minimal door modification. Benefits include:

- **Wireless Communications**
  These systems interact wirelessly, meaning there is no need to install wires at the door.

- **Simple Integration**
  It is easy to integrate these types of solutions into most EAC systems.

- **Simple Access Point Creation**
  New access points can be created within existing or new EAC systems without the necessity of wiring.
  Depending on budgetary restrictions and the specific needs of building owners, managers or users, these different types of system can be adapted and modified to meet defined requirements.

Depending on budgetary restrictions and the specific needs of building owners, managers or users, these different types of system can be adapted and modified to meet defined requirements.
One critical aspect of effective security is that it must anticipate risks and take the most effective measures to mitigate them. For access control, it is no different.

It is important for suppliers of the systems to understand that each safety or security challenge is unique. For this reason, the most effective access control solutions come as a result of collaboration between the supplier, and the customer.

The customer must help the specifier understand how the layout of a building relates to:

- **WHO** can enter a protected area.
- **WHERE** individuals can go within a building.
- **WHEN** individuals can enter a protected area.
- **HOW** an individual can gain entry to a protected area.

The specification team must provide an advisory service. A specifier should explore all available options, and present a number of viable alternatives according to the requirements and budget of the customer.
There is now a huge range of different access control options available to tackle the security challenges that a modern commercial or residential building may face.

This in itself has posed a challenge for time-constrained facilities managers, who face a difficult task identifying the most secure and cost-effective solution.

One way to choose between the different options available is to use one simple planning tool in business, namely the ‘hurdle rate’. This is where specifiers and estate managers work together to answer the following questions:

- How many hurdles or barriers do you need to erect to deter or prevent a risk to security?
- How long do you need each hurdle to deter?
- What is the likelihood of detection and what is the response time on alarm?
- What are the consequences of failure?

With the answers to these questions established, it means that in critical areas it can be perfectly appropriate to invest in several barriers to entry, with clear alarms, response times and routines.

At the same time, there will be other zones, which will not require anywhere near the same hurdle rate to provide an adequate balance between security, risk and cost.

By taking this approach when assessing security requirements, the need to purchase additional security systems can be justified as necessary. At a time when every expense must result in a Return On Investment (either the equivalent in loss prevention or resulting in a premium rental income), this can be a particularly valuable method of specification.
Undermining Access Control

There are a number of factors that may deter an estate or building manager from investing in an access control solution for their property:

Cost
There is still the impression that investing in a new security system has to be a significant capital investment.

Whilst it is true that higher-end, fully integrated systems do have the potential to be expensive, an effective specification should allay this concern. It will help the customer identify a solution that balances security, risk and cost.

Priorities
For some building owners, security is not always the highest priority. However, it is important to remember that the level of security afforded to an individual is a determining factor in the quality of their experience of a building.

As well as this, customers must understand that the cost of installing a quality access control solution can be offset by the cost of what there is to lose. Again, correct specification is essential in situations like this.

Integration
Almost all buildings have some form of security solution in place. The question then for owners or managers is how can access control integrate into an existing system?

Due to the flexibility and wide range of access control systems available, there is a solution for almost every security challenge. As part of the specification procedure, integration will be factored into proposed systems, based on individual requirements.

Personnel
What will the impact be of an access control system on the personnel that need to gain entry to a protected area?

Correctly specified and integrated access control facilitates the secure freedom of movement within a building. With the burden of key management removed, security feels less cumbersome and intrusive for the users of a building.

Access
How does a building owner or manager strike a balance between permissiveness, control and aesthetics, while still identifying the most effective access control system?

Using a hospital as an example, it needs to provide a welcoming and calming environment for patients and staff, while offering adequate protection against the threat of theft and other dangers.

Access control addresses the security challenge for buildings like hospitals, which must secure a space that is intended not only to be a public environment, but a living one.
Summary

The plethora of access control systems available, be they standalone, wireless, or fully integrated, can seem like both a help and a hindrance to time-constrained facilities managers.

For many buildings, it is necessary to strike a balance between creating a welcoming environment, and a secure environment – all the while factoring in budgeting restrictions.

Security planning is concerned with protecting three things: people, assets and data. Access control can deliver this in a cost effective manner, while addressing the specific security requirements of building owners or managers.

With professional specification in partnership with the customer, access control is a powerful tool that will improve security and reduce costs.