

## Are you making your building vulnerable to passers-by?

3 years ago



*Tony Smith, Major Accounts and Marketing Manager at UK manufacturer of entrance control solutions, Integrated Design Limited looks at how entrance control, especially when integrated with other security technologies, can go a long way towards intruder-proofing your building.*

When it comes to securing your building, you can never be too careful. You wouldn't leave your laptop bag on the front seat of your car with your valuables exposed, waiting for an opportunistic passer-by to steal them. So, why would you leave your building exposed to unnecessary risk?

Any obvious weaknesses in your security will make your building and its contents vulnerable to criminals, and may threaten your insurance if you haven't implemented adequate security measures.

There are four major areas where you might be leaving your building unnecessarily exposed:

1. The appearance of inadequate security
2. Actual inadequate security
3. Unsecured internal doors
4. Dishonest or tricked employees

Let's look at these in more detail and consider ways to prevent them.

### 1. The appearance of inadequate security

When scoping a potential target, the first thing to be scrutinised by a criminal will likely be the entrance points, especially if your building is busy with deliveries, staff and visitors all coming and going. They will

consider how difficult it would be to enter the facility undetected, looking at whether you have security guards, a manned reception desk or an entrance control system, for example.

It's important for you to consider what assessment someone looking in from the outside would make about your building at present. If you do not want your building to be open to the public, and potentially criminals with harmful intentions, you need to take steps to ensure that it doesn't look like it is, with adequate visible security in place to dissuade any potential unauthorised entry attempts.

Of course, you don't want your entranceways to appear unwelcoming to authorised users.

Aesthetics and user experience need not be compromised in order to provide the required level of security – you can achieve high levels of security without your users feeling like they're entering Alcatraz!

We've seen a number of our customers, especially those working in high profile public sectors, seeking a highly visible yet still attractive entrance security system. More and more customers are upgrading to full-height barriers, which serve as a strong physical and psychological deterrent, as well as offering reassurance to those working within or visiting buildings.

## 2. Actual inadequate security

Security for security's sake isn't what I'm suggesting, and nor should it just be a vanity thing with you opting for the most impressive-looking solution. It's no good having security measures which look impenetrable, if they don't actually do the job they are intended for.

If you are designing a new security system for your building, you have the opportunity to create something which perfectly suits your requirements. There are many considerations, including the kind of environment you need to protect, the required level of security, the number of people – employees, visitors, temporary contractors – passing through on an average day, whether you want the turnstiles to be manned or not, integrations with other access control and security technologies, available space, design style, budget...the list is long.

Often, however, organisations don't have the opportunity to design their own, instead inheriting a legacy security system when they move into a building. If the system wasn't specifically designed with your requirements in mind, this can quickly lead to frustration, which often results in users and operators of the system purposefully bypassing it by manually opening a lane to allow multiple users to pass through at peak times to avoid delays to their working day. The risk in this scenario is clear.

## 3. Unsecured internal doors

When designing an entrance control system, the focus is often only on securing the main entry points, such as the lobby, reception areas, staff entrances etc. Whilst securing these points is vital, you also need to consider adequate protection for your internal spaces, such as your data centre or HR office, which may be critical to the functioning of your organisation or house sensitive data which you wouldn't want falling into the wrong hands."

Having a bank of security turnstiles at the front door will prevent unknown individuals from entering the building beyond reception, but won't prevent authorised individuals within your organisation – or approved external contractors such as service engineers or cleaners – from being able to access more sensitive

areas of the facility. No matter how rigorous your background checks, a belt and braces approach is the most effective way to minimise opportunistic crime.

#### 4. Dishonest or tricked employees

You might have a robust, fit-for-purpose security system installed but, if your employees don't understand its importance and aren't clear on your security protocols, they could leave your building exposed unknowingly.

Traditionally, one major danger is 'tailgating' - the act of following someone through an open door or turnstile unauthorised. The follower is the one at fault, even if there is no intent to deceive or cause harm, and the person being followed may not even be aware of the act.

In contrast to innocent tailgating, 'collusion' is when individuals purposefully act to let someone in through a secured point who otherwise wouldn't gain access. With collusion between those entering, the one with the approved credentials is at fault, as the intention is to bypass the security system to allow unauthorised access.

The threat that arises through collusion involving staff should not be underestimated, including unintentional collusion, such as 'being kind' and letting someone they believe is harmless through a controlled access point because they "forgot their key card".

These are just four of the most common factors which may be putting your building at risk from opportunistic passers-by.