Improving Security In The Built Environment

by Gavin Jones, director of SABRE at BRE Global

In recent years, the threats affecting businesses and the built environment have changed dramatically, both in intensity and diversity, and they continue to do so.

There is not a day that goes by without the media reporting on terrorism or cyber attacks targeted at society, institutions and companies. Terrorism by its very nature is highly visible and can make people feel very vulnerable when they are in public places, at work or staying away from home.

Undoubtedly, this anxiety has made end users and a range of professionals involved in the design, procurement and management of buildings and infrastructure ask many more security related questions. Questions such as:

- Are we a target?
- Are we secure?
- Should we install CCTV, fences or deploy additional guards?
- Do we need to invest more in security?

Generally, these people are looking for some level of reassurance. They want to know what others are doing:

- Are they changing the way they secure their facilities?
- Are they spending more on security?
- What innovative solutions are available to address these emerging threats?

Ultimately, these people do not want to fall behind their peers. This in itself can make their estate a more attractive target and them as individuals personally liable where failings are identified in security following an incident. This is all very understandable.

Unfortunately, these questions are largely coming from people at the coalface, people that can implement better security but only when they are able to access appropriate resources to facilitate improvements. Sadly, there has been little evidence of a substantial change in the level of resources available for facility security managers in response to increasing threat.

Generally speaking, these people will be representing one of two types of enterprise, those that are:

- Security conscious i.e. organisations that inherently value security due to the nature of their business and are therefore willing to invest; or
- Indifferent towards security e.g. organisations that do not necessarily see a link between security and the success of their business and therefore ask: “Why should I invest?”

Understandably, business leaders have a range of competing issues to address to make their businesses successful. However, if a business wants to be secure, it needs to ask for security and fund it. This needs to come from the top in the form of a commitment to operate securely for the benefit of staff, customers and other stakeholders. In some sectors, such as energy, aviation and communications, this is par for the course. Senior executives will know that if they fail to establish effective policy, comply with regulations and give stakeholders confidence in their ability to operate safely and securely, they will not have a business and will struggle to attract custom and investment. In these environments, it is essential to establish a security culture as security is core to the success of the business.

You can recognise these businesses by looking at corporate strategy and business financial reporting. Security will feature in strategic priorities and when setting out principal business risks and uncertainties. Today, as before, these are the businesses that will be best placed to weather the storm. In the other camp, security is not traditionally recognised as a core factor in determining business success. Financial reports for these businesses will focus on profit and loss but not security. These businesses were probably vulnerable before and will remain vulnerable. However, now that the threat has increased, so have the risks to their business.

The big question today is, regardless of the nature of a business, can any organisation afford to ignore the business risks associated with today’s security threats?

All businesses, from SMEs to large corporates, need to be security conscious for a range of reasons, including:

- Rapid communication of incidents via traditional media outlets and social media that can impact reputation;
- High consumer expectations versus a just-in-time approach to manufacturing and delivery of services, which can quickly damage confidence when things go wrong; and
- Health and safety legislation and data protection requirements which apply to all.

As a result, security performance, like business finances, should be monitored, assessed, evaluated and reported. This will require a change in many boardrooms; unfortunately many organisations are unlikely to change until they see further examples of reputational damage, lost earnings and eroded trust in their sectors or even in their own business.

So if you are a facility or security manager, and you are not feeling pressure from above to react to the new security reality, what is this likely to mean?

Well, you are probably wondering what you can do, if anything. If you have considered ramping up your facility's security, you are probably struggling to get additional resources to implement your plans and even if you try, you may face push back from end users. Fundamentally, very little will change at a local level without enterprise direction and support, regardless of the security context.

So how should you proceed?

The following points apply whichever type of organisation you represent. They will help you assess your current situation and what might need to be done in the future.

Understand your security needs

- What assets do you have at your facility?
- How much security can you realistically implement without impacting on operations?
- Who uses your facility, when and what level of access is required?
- Do you have obligations to any 3rd parties?

Understand the risks

- What threats are relevant to your type(s) of facility?
- How does the geographical location and local setting influence the likelihood of an incident?
- Is your facility iconic or does it have attributes that make it an attractive target?
- Who might attack you, when and how?
- How vulnerable is the facility to these types of incidents?
- What consequences may result in the event of an incident(s)?

Through the analysis of these issues, you will be in a position to determine whether any action is required or at least if further assessment is necessary. If you have not considered these factors, then there can be little assurance that your facility security is effective or that any planned investment will deliver tangible improvements.

This information can be used to communicate local issues to senior management. Risk communication will assist you in making a case for improvement and in some cases may even highlight cost savings if existing measures do not contribute to better security outcomes.

What security improvements should you implement?

There is no silver bullet to address the likes of 'lone wolf' attacks and the police certainly cannot be everywhere, all of the time. Your approach to securing your facility will naturally be dependent on the results of the risk assessment. The measures you adopt should be focused on reducing vulnerabilities and consequences i.e. improved protection. Never implement security for security's sake. It is disappointing to see significant investment in measures that do not translate into improved security. This can result in a false sense of security for the occupiers and is purely security theatre. In some cases, it may be possible to deter certain types of crime through visible security features but it will be difficult to evidence their value. Remember, if in doubt, you should always seek professional advice.

At BRE Global, our experience in supporting organisations to improve their physical security has identified a number of characteristics that are evidenced when we witness effective facility security:

'A strategic approach'

You should have a written policy and a supporting security strategy which set out what you are trying to achieve and ensure that security measures meet operational requirements. This will allow you to remain focused on your objectives and ultimately measure performance.

'An integrated approach'

You must be careful not to solely focus on physical and technical security features that could quickly absorb your entire security budget. Recent events have shown how quickly threat can change. How you might be attacked tomorrow may be very different to the methods used in recent attacks. Criminals and extremists have shown that they can use very simple tactics to achieve their goals or embark on complex organised cyber attacks which the average person may not even understand, let alone anticipate ahead of time.

Our built environment is traditionally slow to adapt, with physical changes being time-consuming, expensive and disruptive to implement. It is important to achieve balance by integrating personnel security, cyber security and physical security. This requires leadership, cooperation and coordination.

'A Risk Management System'

Establishing a security risk management system will help you get the most out of your security budget. It will provide a framework for effective security and enable you to evidence the steps you have taken to mitigate risks. In a security conscious organisation, there may be an enterprise level risk management system. In this case, your local management system should be aligned with that of the organisation. Where this is not the case, you may wish to establish your own system.

'Tried and tested incident management & recovery plans'

Far too often, security planning stops at the point of incident detection or an incident plan may rely solely on the police for incident response. It is important that, having detected suspicious behaviour or a loss at the facility, there is appropriate infrastructure and procedures in place to communicate with interested parties and manage an incident to a successful conclusion. This might require on-site personnel to take response and recovery actions in order to mitigate losses.

Having invested significant time and resources in mitigating security risks, it is important that you are able to communicate your facility's security credentials and provide stakeholders with assurance of your capability. This might be required internally within some organisations, it may be a regulatory requirement for your sector or act as a differentiator that offers competitive advantage.

The solution

BRE Global has developed SABRE, a new security assessment and certification scheme to provide this assurance. SABRE certification of a facility allows stakeholders to compare, measure and improve security performance, and determine what security improvements offer best value for money. We will be at the UK Security Expo on 30th November and 1st December 2016 to launch SABRE to the market.

If you would like to know more about SABRE assurance ratings and how your organisation can benefit, please visit www.bre.co.uk/sabre or contact us at SABRE@bre.co.uk.

ENDS