ProtectUK

Tactic DB4: Ensure that visitors and contractors are accompanied at all times

ProtectUK publication date

14/12/2023

Information and Intention

It is the employing organisation which owns and needs to effectively manage the risk of granting visitor and contractor access to its sites and assets, not the contractor organisation or agency or, indeed, the visitor themselves. Whilst on the premises, you have a duty of care to the visitor and/or contractor. As a result, all visitors and contractors accessing the premises should be accompanied at all times.

This process provides audit information, including sign-in/out times, who accompanied the visitor/contractor as well as the purpose of the visit. This can be crucial in the event of an emergency evacuation of the premises.

The organisation has a responsibility to ensure good security practices are in place and are followed by all those who access their premises. In many organisations, the traditional approach to security has focused on addressing physical and information security issues. The people element, which is equally important, has often been overlooked. The actions and attitudes of people can make all the difference.

A significant factor affecting how people act is the security culture of the organisation. This can be defined as the styles, approaches, and values that the organisation wishes to adopt towards security.

In organisations with a strong security culture, employees, contractors and visitors will tend to think and act in a more security conscious manner, helping reduce risk and vulnerability, which in turn helps protect against reputational damage, business impact and ultimately national security threats. Effective security measures can help to create a controlled environment which will encourage positive security behaviours amongst staff, visitors and contractors, act as a deterrent and protect from

criminality, including terrorism.

Threat actors may rely on the cooperation and assistance of an ‘insider’ within your organisation. An insider could be a new or existing full-time employee, a contractor, visitor or agency staff. Without having someone working from within, those who threaten may find it difficult to access secure areas within the organisation. Companies could be targeted deliberately, where the insider will seek access in order to exploit the organisation. The process of escorting visitors/contractors may help to mitigate the risk of a potential insider threat.

Method

Having been signed into the premises and allocated passes, visitors and contractors should be escorted throughout their time on the premises. If the contractor requires to remain on the premises for extended periods, additional checks may be undertaken, thus negating the need for permanent escort. Identification passes should be worn and be visible at all times.

By implementing effective personnel security procedures (see Good Practice Guide for Employers) in respect of visitors and contractors, you will:

- Reduce the risk of allowing access to visitors and contractors who are likely to present a security concern.
- Minimise the likelihood of visitors and contractors becoming a security concern.
- Reduce the risk of insider activity, protect assets and, where necessary, carry out investigations to resolve suspicions or provide evidence for potential criminal/disciplinary procedures.
- Implement security measures in a way that is proportionate to the risk.
- Reduce any potential risks to the contractor and visitor.

Administration

Policy and procedures should mention the requirement to ensure that visitors and contractors are accompanied at all times whilst accessing the premises. Identify ownership of the policy and governance of the decision making, including who is responsible for the management, coordination and strict compliance, together with the relevant record keeping, and how its effectiveness is assured.

Ensure staff understand processes and procedures to be adopted, including actions and contingencies.

Risk Assessment

Three types of people and their roles need to be considered:

- Security personnel
- Front-line staff, including contractors (see Contract Staff)
- Members of the public – this concerns providing information and guidance to people visiting your site on how to protect themselves should an incident arise or to recognise an attack is under way. This can include various types of communication such as posters, announcements, signs etc.

A risk assessment should identify threats which could have an impact on the business and recognise any existing vulnerabilities. Risk assessments should clearly define a duty of care to staff and others on both an organisational and individual level.

Staff and visitors may have different responses to the same incident and therefore you should risk manage the impact of staff, contractors and/or visitors, as well as members of the public, not following or directly contradicting instructions.

For further information see Advice for security managers during a heightened threat level and Security risk management.

Consider cancelling non-urgent business or visitors where appropriate.

Communications

Internal Stakeholder Engagement:

Certain aspects of visitor and contractor attendance may not necessarily be communicated to all your staff. However, staff members should be briefed on what to do with regards to their presence on site and should they observe suspicious activity, they should be encouraged to identify and report any suspicious activity or item they observe, or that they know about.

It is necessary to ensure points of contact are known to staff internally, and partners externally. Any information regarding the escort of visitors and contractors should be disseminated internally through the communications function.

All security management/security staff should understand this process and what is required of them, in this regard. Internal communications should encourage security awareness by general staff and a

positive security culture should be encouraged through internal communications.

You must provide information for your staff so that they can help deliver on the security plan. Your internal audience will inevitably cross over into your external audience, so consider what messages you want them to share with external networks, e.g. families and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

Engagement with neighbouring businesses should include basic information regarding changes to security practices if it impacts on neighbours. However, specific information on such processes should not be shared externally.

Early identification and engagement with key external stakeholders are important. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering the plan, and consideration should be given to engaging with any working groups or for a who may already have identified ‘best practices’ and lessons learned from similar sites within the business area the site operates within.

There are a number of key principles that should be applied when engaging with stakeholders:

- The engagement should be different for different stakeholders, at different times – it should be flexible as one type of engagement process does not necessarily suit all stakeholders.
- It should be a two-way engagement process, where information and knowledge are shared.
- Communications should be genuine and timely, where there is the ability to influence outcomes, dependent on feedback.
- Engagement with stakeholders should be open and transparent.

As with all matters relating to security and policing, the relationships with the police are key. The contact may be with either the local police or those specifically tasked with providing policing to certain sites.

External Media Engagement:

Engagement with the media should be encouraged to allow a positive and deterrent message to be disseminated to the general public, as part of the Security-Minded Communications strategy.

By positively reinforcing a security deterrence message, it is likely that this may deter potential attackers when they carry out online hostile reconnaissance as part of the attack planning process.

Health and Safety/Other Legal Issues

The protection of visitors and contractors at a location is governed by legislation, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- The Fire Safety Order 2005
- The Fire (Scotland) Act 2005
- Employment Rights Act 1996

It is important to consider any security measures as they relate to visitors and contractors, with regards to justification, proportionality, necessity and legality.

You should ensure that there are well-defined governance arrangements and that records are kept of the issues, decisions made and the reasoning behind those decisions which involve visitors and contractors. Records will provide evidence to any investigations, or public enquiries, and assist in defending against legal action, criminal charges or civil claims.

The importance of keeping accurate records and having well defined governance arrangements has been demonstrated during the Manchester Arena Inquiry.

Accompanying visitors and contractors at all times must include consideration of relevant legislation as well as details of your organisation’s insurance policies. Consideration must be given regarding the personal health and safety of staff in the performance of their duties.

KEYWORDS
THREAT
SECURITY MEASURES
SECURITY MINDEDNESS
RISK ASSESSMENT