ProtectUK

Tactic VB1: Ensure a strong security posture through Security Minded Communications

ProtectUK publication date
14/12/2023

Information and Intention

Security-Minded Communications (SMC) is designed to equip organisations that manage sites, venues and events with the ability to utilise communications as part of their protective security measures.

Those planning an attack will typically conduct hostile reconnaissance to gather key information.

A good Security-Minded Communications strategy will help deter attackers from selecting the organisation, site or event as a target in the first instance because:

- They are unable to get the information they need online.
- They are concerned about the effective security measures that are in place at the venue.

Similarly, it will inform and reassure regular users by:

- Demonstrating what is being done to maintain the ongoing safety and security of staff and visitors.
- Encouraging staff and visitors to remain vigilant and assist with security and reporting suspicious behaviour.

Security Minded Communications is quick and easy to put in place. It can be integrated into existing security and communication plans, and provides numerous benefits for organisation and venues, including:

- Adding another layer of security at no or low cost.
- Enhancing customer service by making your customers and visitors feel safe.
- Reducing potential vulnerabilities.
- Denying hostile access to information that they require for attack planning.

For more information see [ProtectUK - Communication - Security Minded Communications].

Method

Security-Minded Communications is designed to disrupt hostiles during the reconnaissance stage of their attack planning, making it less likely that they will choose your organisation, venue or event as a target for an attack. It has been informed by an extensive research programme and can help to equip organisations, venues and events with the ability to use communications as part of their protective security measures.

Hostiles may have differing objectives, but there are identified similarities in their planning approaches. Research
shows that there are three stages in a hostile's attack planning:

1. Target identification;
2. Detailed planning; and
3. Planning confirmation and action.

A key part of the first two stages is hostile reconnaissance. The National Protective Security Authority (NPSA) defines hostile reconnaissance as "purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target".

A hostile does not need to physically visit a site to obtain the information they require. They can use online resources to gather useful and current information from credible sources. Looking at communications through the eyes of a hostile can be the most effective way of understanding hostile behaviour. NPSA research has found that communications from and about an organisation, venue or event can encourage or discourage hostile planning activity.

Security-Minded Communications aims to help protect an organisation, venue or event by viewing existing and planned communications through the eyes of someone who is seeking to gather information to help them plan a hostile act against it.

When creating Security Minded Communications content, you should consider:

- What do I need to communicate?
- How can I use this opportunity to include messages that could deter a hostile?
- How can I ensure I provide information without giving away details that would be potentially useful to a hostile?
- If I need to publish detailed information, how can I counter any vulnerability created by promoting the protective security measures in place?

By applying this approach, you make your venue less attractive to potential attackers and potentially divert their attention elsewhere. For further information, see ProtectUK - Make Security-Minded Communications part of your security plans.

Finally, you can take steps to mitigate the impact of an attack by preparing a crisis communications plan (TACTIC EB4). NPSA has partnered with the Chartered Institute of Public Relations (CIPR) to deliver best practice guidance for communications professionals on the preparation and management of threats from hostile actors.

Administration

Deterrence/Security Minded Communications should be developed, tested, and refined to ensure it will protect people as intended. This should form part of an Emergency Response Plan, designed using the 'deter, detect, delay' principles. Further details of what should be included in an Emergency Response Plan can be found on Protect UK.

Policy and procedures should mention Security Minded Communications if the threat level is raised. You should identify ownership of its deployment and governance of the decision making. This includes who is responsible for the management, coordination and strict compliance, together with the relevant records keeping, and how its effectiveness is assured. Ensure staff understand processes and procedures to be adopted, including actions and contingencies.

Keeping records of what you are aiming to achieve through a Security Minded Communications Plan, and why/how it will be implemented, procedures to be followed and the outcomes of tests and rehearsals will assist your planning and refinement process.

Risk Assessment

A risk assessment should identify threats which could have an impact on the business and its vulnerabilities. This risk assessment can be used to define the actions that are required regarding the use of a Security Minded Communications strategy. Such risk assessments should clearly define organisational as well as individual duty of care to staff and others.

For terrorist-related incidents, reputational damage will be caused if the organisation handles the issue badly. For example, communicating insensitively, poorly, or not at all. In addition to reputational risk, a failure of Deterrence/Security Minded Communications and successful exploitation of vulnerabilities by terrorists could lead to loss of life or serious physical damage to the site and these risks must also be acknowledged. It is important to record current and emerging risks, risk management and mitigation measures, reminding those under your charge of their duty of care to themselves and others.

Communications

Early identification and engagement with internal and external stakeholders are important at each stage of the development of a ‘Security Minded Communications’ strategy, from assessing the risk, through to developing appropriate responses. Agreement must be sought in relation to the roles and responsibilities of all those involved.

Internal Stakeholder Engagement:

In the event of a Security Minded Communications initiative at your site, it is essential that this information is communicated to your staff, and that they know what to do should suspicious activity be detected.

It is necessary to ensure points of contact are known to staff internally, and partners externally. The most appropriate terminology should be employed, namely ‘Security Minded Communications’, and the concept should be understood by everyone. This could be achieved internally through the Communications function. Use should be made of media and external stakeholder to amplify the deterrence message.

Further information on security minded communications can be found on the NPSA website, via the guidance document: NPSA - Security-Minded Communications Official Guidance - 5 Minute Read.

You must provide information for your staff so that they can help deliver the plan. Your internal audience will inevitably cross over into your external audience so you should consider the messages you wish these individuals to communicate messages to their external networks e.g. families, and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

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 forums 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

Businesses/organisations that are developing Security Minded Communications plans should ensure that all activities are assessed in line with Health and Safety and other legal/policy frameworks, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- Employment Rights Act 1996

It is important to consider any SMC related activities with regards to justification, proportionality, necessity and legality. Incorrectly identifying a member of the public as a potential ‘hostile’ could lead to legal issues and all options should be considered as potential mitigation measures in the risk assessment process.

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 SMC related incidents. Records will provide evidence to any investigations, or public enquiries and assist in defending against legal action, criminal charges or civil claims.

KEYWORDS
SECURITY MEASURES
SECURITY MINDEDNESS
COMMUNICATIONS
HOSTILE
EMERGENCY PLANNING