ProtectUK

Tactic EB4: Ensure a Crisis Communication Plan is agreed and document all decisions including rationale

ProtectUK publication date

14/12/2023

Information and Intention

Ensuring that any identified plan is agreed, and all decisions are documented, including rationale, will ensure consistency and clear lines of responsibility for the management of an increased period of threat or incident.

By planning in advance and having relationships and initial key outputs in place, organisations can ensure they are taking a leadership position as soon as a crisis occurs. Recent high-profile incidents have moved security higher up the agenda for organisations. Transport hubs, energy infrastructure and areas that host large public events and gatherings, from shopping malls to stadia and arenas, are all potential targets.

These events have changed public perception. People are more accepting of security measures such as bag checks, surveillance and an increase in visible security staff. There is an expectation that these measures exist and that organisations are prepared for the worst. In a world of rolling news coverage, social media and citizen journalism, businesses are scrutinized more than ever.

Communication has never been more important, both in terms of deterrence and how organisations react to a crisis. 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. Alternatively, for something like a cyber-attack, the organisation's IT policies and security will be examined, and they are more likely to be held responsible.

Method

The overall business strategy in dealing with an increase in threat level or in response to an attack is:

To understand the type of threat posed – Why did the threat level increase? What was the attack methodology used?

To consider the appropriate level of response and range of tactical options that are best suited to continue business-as-usual, in the parameters of this heightened state of alert.

Therefore, you should ensure your Crisis Communication Plan is agreed, in order to assist maintaining critical and urgent business activities and the work your business must continue to do, to survive the disruption from an increased period of threat or terrorist attack.

Further information on leadership and governance can be found on the NPSA website: NPSA - Leadership and Governance.

It is important that the communications team is aligned with operations within the business and key decision makers, from management through to key department heads, and that security culture has been built and is consistently reinforced. The organisation should enhance and further develop existing relationships with strategic partners (e.g. police and other emergency services), ensuring the Crisis Communication Plan is in place including a policy relative to a Menu of Tactical Options (MoTO), holding statements (including provision for following the police lead), roles and responsibilities, and resources.

By planning well, practicing frequently and having in place a coordinated effort, as well as understanding the vital role of strategic communications, a crisis can be well handled and well communicated. Communicating bad news well is now expected of all major organisations.

As the result of actions of a hostile actor, the police will have the lead role in communicating to external audiences in an effective and timely fashion. However, the target organisation will remain important and should reinforce messaging and ensure that consistency and accuracy are maintained.

If the police, or government department are not the designated point of contact for the media, the organisation should act quickly to take the lead, and position itself as a source of truth.

Administration

A single accountable board level owner of security risk and a top-down implementation of security policies and expected behaviours is likely to promote a more compliant and consistent approach across your organisation/business.

You should make sure that someone is given explicit responsibility for any improvements identified and putting any additional control measures in place. This person should have sufficient authority to

make sure that the necessary resources and money are made available.

For further information see ProtectUK: Risk Management Process – Record your Decisions and Actions.

The Crisis Communication Plan should be reviewed at pre-agreed intervals with interested parties.

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 issues that need to be addressed – either to prevent them from affecting the organisation, or detect them if they have already manifested themselves. As such, ensure communications are continuing to monitor feedback and have an active listening role.

The perception may be that the organisation was lacking and therefore was weakened before the incident occurred; this is particularly the case for cyber incidents. Such risk assessments should clearly define organisational as well as individual duty of care to staff and others.

Staff, contractors 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.

Communications

Internal Stakeholder Engagement:

Dedicated channels should be established, with backups if access to the organisation's intranet or message channels is limited (for example if the intranet is restricted due to criminal investigations), if the network is overloaded, or if it has been the target of the attack.

You must provide regular 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 you should consider the messages you want them to convey 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:

Engagement with neighbouring businesses (see TACTIC IB4) should include information regarding the Crisis Communication Plan if it impacts on neighbours. However, certain specific information regarding internal communications 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 communication strategy, 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:

After a terrorist incident has occurred, organisations should not communicate directly with the media or external audiences on anything related to the incident, without prior consultation and agreement with the police. In addition, avoid revealing details about the incident through social media without prior police consultation.

An appropriate individual should be identified in the organisation to liaise with the police in order to disseminate approved information which is accurate, and which will not compromise the criminal investigation.

However, general 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 should ensure that the Crisis Communication Plan is assessed in line with

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 Crisis Communication Plan 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 communications. 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.

Communication strategies must include consideration of relevant legislation as well as details of your organisations insurance policies. Consideration must be given regarding the personal health and safety of security staff in the performance of their duties.

KEYWORDS
STAFF
RISK MANAGEMENT
RISK ASSESSMENT
COMMUNICATIONS
SECURITY
SECURITY PLAN