INTELLIGENCE BULLETIN

1st July 2019

Securitas Intelligence Unit

A "SCaN" a day to keep the hostiles away

Information, information, information........ when your organisation becomes target for criminal activity, information is what they need. If you have not considered yourself to be open to hostile reconnaissance, then you are more likely to be providing this information to criminals too easily. Simple steps can be taken to reduce this threat to your business as usual.

The City of London Police backed up by guidance from the Centre for the Protection of National Infrastructure (CPNI) have developed an awareness program for business security aimed at identification, denial and detection of hostile reconnaissance.

Their programme is called **SCaN**:

See ⟶ **C**heck ⟶ **A**nd **N**otify

Hostile reconnaissance is a research method commonly associated with terror threats and extremism however, in recent times it has become evident that hostile reconnaissance is used more widely than is commonly believed.

Be it criminal organisations who wish to commit crime against a business, protest activists who require their short term activities to have a longer term impact or urban climbers whose aim is the challenge of your buildings – completion of hostile reconnaissance in advance of activity can ensure the maximum benefit is obtained for those involved.

During hostile reconnaissance, information covering the state and patterns of security at a site, the chances of being detected, the vulnerabilities of security and the best method to achieve success are researched by the operative. This information is utilised to plan and formulate the disruptive 'attack' in order for efforts to be rewarding.

A wider meaning to hostile reconnaissance

A well-developed tactic for criminals and activists

Ignoring possibilities could be costly

If you would like any further information on any of the elements mentioned in this bulletin, please email the Securitas Intelligence Unit at soc.intelligence@securitas.uk.com

In many cases training that covers hostile reconnaissance uses the term 'attack', focusing the audience upon the most serious of offending. Memories of terror atrocities across the world are often drawn upon as examples of hostile reconnaissance.

By using the word 'attack' are we focusing the minds of our decision makers, security managers and front-line teams upon terror and extremism? Are we at risk of missing the point that hostile reconnaissance on a lower level can cause significant disruption and serious harm to an organisation?

Successful hostile reconnaissance can result in long term implications to business as usual, increased cost and significant brand impact depending upon the aim and actions of those involved.

The "SCaN" program identifies three opportunities for security and operations teams at all levels to disrupt hostile reconnaissance.

1. **DETER**
2. **DENY & DETECT**
3. **MITIGATE & RECOVER**

Whilst these terms are generalised it appears that they are suitable for all organisations if applied to individual circumstances.

DETER – deter the hostile reconnaissance operative (HRO) at target selection. Make your target too difficult. Ensure the perception is that your site is more challenging than a similar one elsewhere which would suit the HRO campaign. Ensure there would be minimal reward from any activity completed at your site.

In practice this could be a combination of technical, physical and personnel measures. Varying security protection ensures that patterns cannot be easily identified by a HRO. Conducting penetration testing of operational systems and teams can reduce complacency. It also instils confidence in teams to identify, challenge and question activity which may be associated to a HRO.

DENY & DETECT – HRO is detected by the efficient and robust security procedures you have in place. Front line teams must aware of possible risks to your specific organisation and trained to look out for them.

Once challenged, ensure a fast time reporting methodology is in place with escalation to decision makers for urgent and immediate review. Front line teams need to know they will to be listened to. Gather information about the modus operandi used by the HRO. If you operate across multiple sites, information about the modus operandi used by the HRO is essential for dissemination across your assets.

MITIGATE & RECOVER – following identification of a HRO and their suspected line of activity ensure timely and appropriate measures are put in place to prevent a security incident. These could be physical, operational or ad hoc in order to mitigate any further HRO activity.

For example – if protest activity threatens your business as usual ensure you have insight into methods used by the protestors in order to remove this tactic as an option for them. Utilising physical measures, increased patrols, and even engagement with protest groups can reduce and mitigate the impact on your business as usual.

Organisations are recommended to consider their vulnerability to hostile reconnaissance at all organisational levels and beyond physical security. The SCaN methodology should be considered more widely against loss of commercial data and insider threat. Training, mentoring and workshops tailored to each role can increase identification of suspicious activity, drive confidence in staff and encourage a more customer focused experience. Or as the City of London Police suggest "The Power of Hello".