Securitas Intelligence Unit

Advisory report: Security Auditors

17 May 2021

Intelligence@securitas.uk.com

This report is subject to GDPR and data retention policies in line with such regulations.

Securitas provides the intelligence reports for the recipient's business internal use. Securitas accepts no responsibility for any decisions taken by the recipient on the basis of the analysis offered in this report. Use of Securitas' name, brand names, logos, taglines, slogans, or other trademarks without written permission is strictly prohibited. Disclosing, copying, distributing or use of any part of the reports electronically or otherwise other than for the strict purpose for which it has been provided is strictly prohibited. Securitas Security Services (UK) Limited is a limited company registered in England & Wales. Registered number: 01146486. Registered Office: St James House, 13 Kensington Square, London, W8 5HD © Securitas Security

Priority Intelligence

- **'Security auditors' are activists who film public and private organisations, from a 'public space', for varying reasons, primarily to raise awareness of their rights and freedoms, but also to challenge the establishment, law enforcement and government powers, and promote conspiracy theories.**
- **Auditing has gathered significant support in recent years, further fuelled by anti-establishment sentiment during the pandemic and anti-police movements throughout 2020-21, with a growing number of activists using auditing techniques to raise awareness of their cause(s), in addition to the rise in civilian journalism.**
- **The Securitas Intelligence Unit assesses that trends in auditing will likely increase due to its popularity as a form of raising awareness of civil rights. Additionally, the use of auditing could be adopted by activist groups to form an additional dimension to protest tactics.**

Situation in detail

Background

'Security auditing' first emerged in the US as part of the 'First Amendment Audit' movement, a form of activism centred around the constitutional right for members of the public to freely film and photograph public spaces.

Auditing is also linked to the Photography Is Not A Crime movement (PINAC) movement (started by a group of the same name, which has spread internationally), which campaigns in support of press freedoms, free speech, and oppression of these rights, typically by police officers.

In context of businesses, security auditors record organisations (property, premises and people) to promote their rights and freedoms, and to provoke a security response, but also to raise awareness of perceived business faults, such as corruption, unethical business practices and climate change.

Auditing vs activism

Practitioners often refer to themselves as auditors, whose intentions are to promote civil and human rights, freedoms, and government transparency; however, some activists engage in auditing to raise awareness of activism and various causes, such as police brutality. Additionally, conspiracy theorists, are increasingly promoting and adopting the use of security auditing in an effort to 'expose the truth'.

Auditors target both private and public organisations (see: Modus Operandi – Targets below). They position themselves on public property, such as a footpath, and begin recording their target, including premises, property, and people.

While the primary aim of the majority of auditors is to raise awareness of the cause (i.e. civil and human rights), some practitioners intend to provoke a security response to be captured on camera.

Whilst the first amendment does not apply in the UK, auditing has grown increasingly popular with anti-authority and anti-government movements, particularly since the start of the COVID-19 pandemic, where significant restrictions were implemented to prevent the spread of the virus, leading some groups to accuse institutions of infringing on civil liberties.

The legality of auditing

According to UK law, there is no provision allowing police to arrest and charge auditors in public spaces, unless there is a reasonable suspicion of an offence being committed, usually related to terrorist activities or trespass.

With regards to terror related activities, recording / photographing in public spaces could be interpreted as hostile reconnaissance or intelligence gathering, specifically the photographing of 'soft' targets, specific buildings or locations, CCTV, entry / exit points, crowd numbers and security details. However, in busier locations, such activity could also be incidentally captured by those looking to film / photograph buildings for other reasons, such as tourism or an interest in architecture. This provides an additional layer of challenge to security officers / law enforcement attempting to separate genuine threats from incidental and / or 'nuisance' interactions.

The Terrorism Act 2000 provides law enforcement with the necessary provisions to stop and search an individual suspected of being a terrorist. Equally, law enforcement can arrest an individual that has acquired, published, or communicated sensitive information relating to armed forces members, police officers and intelligence service members that could be used in committing or preparing an act of terrorism. However, there are no such provisions enabling private security staff to detain, confiscate or otherwise demand access to photography / recording equipment.

Recent UK auditing activity and trends

One of the most common and active UK based auditing movements is Auditing Britain (AB); a one-man YouTube channel with nearly 100,000 subscribers and hundreds of thousands of views per video. AB has recently attended public spaces outside of police stations, COVID-19 testing sites and banking institutions.

- In July 2020, AB attended an area outside Cambridge Police Station and began filming officers and vehicles entering / leaving the site. When approached by police, AB immediately cited their legal rights to film in public spaces. The discussions between the cameraman and the police quickly escalated after allegations of police assault, to which the cameraman entered the police station and attempted to file a complaint.
- In October 2020, AB attended a COVID-19 test site in Oxford and began filming the site from a public space. Security confronted AB resulting in a heated interaction and security notifying the police of potential hostile reconnaissance.
- In April 2021, AB attended the entrance (deemed a public space) to a banking institution in Derby and began recording the employees and customers. Employees alerted the police of potential hostile reconnaissance to which police attended the scene and questioned AB.

Auditor (AB) filming a COVID-19 test centre.

Auditor Modus Operandi

Targets

Typical auditor targets include (but are not limited to):

- **Aerospace and defence.**
- **Capital projects and infrastructure.**
- **Engineering and construction.**
- **Government and public services:** police stations, prisons and custody centres, NHS facilities, fire stations, council offices and facilities, military assets including bases, installations, and temporary / mobile assets.

The pandemic has fuelled conspiracy theories across the globe and provided an opportunity for theorists to target individuals and organisations they perceive to be linked to COVID-19 being a hoax. This includes organisations accused of establishing and upholding the regulations such as government buildings and retail sites. Auditors have targeted COVID-19 test / vaccination centres and hospitals, allowing for further engagement with likeminded individuals within the online community.

Auditor filming outside RAF Benson.

However, anti-lockdown / anti-vaxx activists are increasingly targeting a variety of industries and sectors who they perceive are at fault as part of the COVID-19 pandemic and response. As such these industries and sectors may be targeted by auditors, or anti-lockdown /anti-vaxx activists, including:

- **Healthcare:** hospitals, local GPs and medical centres, and COVID-19 testing and vaccine facilities.
- **Pharmaceuticals and life sciences:** pharmaceuticals including organisations involved in development / manufacture of therapies (i.e. drug treatments, testing equipment, medical hardware, vaccines) etc.
- **Media and entertainment.**
- **Retail and consumer:** shops, shopping centres and supermarkets (face masks)
- **Technology.**
- **Telecommunications:** 5G.
- **Transportation:** transport hubs (airports, bus centres etc.)

Ultimately, as with all forms of protest related activity, any organisation could be targeted by specific groups / individuals, utilising auditor tactics, techniques, and procedures (TTPs), either as part of an isolated event, or during a wider event (i.e. a demonstration). Examples of this include environmental activists filming recent demonstrations targeting oil and gas organisations, and financial services.

Tactics, techniques, and procedures (TTPs)

Reconnaissance: Auditors are not typically opportunistic and will often complete some form of reconnaissance of a target prior to engagement. Auditors observe the layout of the target – its entry and exit points, availability and distance of public spaces and type of employees likely to engage with.

In the post-reconnaissance phase, some auditors may post photographs of the upcoming target as a way of communicating with their audience and keep them informed of future videos. However, the majority of auditors will circumvent this in favour of maintaining an element of surprise.

Auditing: Some auditors may begin recording prior to arriving at the target location in order to introduce viewers, such as the location and objectives. Having predetermined the appropriate public space, the auditor will then proceed to occupy the space and begin filming the building / facility, entrances, exits and members of staff.

Common public spaces occupied by auditors include:

- Pavements.
- Roadsides.
- Entrances / exits to buildings and sites.

Some auditors are adept at occupying what may initially appear to be private spaces but are actually public. This highlights the extent of research undertaken by auditors, such as analysing public ordnance surveys to determine the ideal space to occupy.

Filming outside HMP Leeds.

Recording is often done overtly, using standard photography equipment or a mobile phone, however some activists also record covertly, using discrete or disguised equipment in the form of body worn cameras.

A prevalent auditing belief is by recording interactions, the auditor will have more control over the situation and to an extent, the target individual's actions and responses. In other words, individuals confronted with auditors are perceived to be less likely to act in a confrontational manner if they are aware they are being recorded for fear of legal repercussion. However, some auditors specifically seek a hostile or confrontational reaction from the individuals they encounter, as it yields more captivating material for their viewers.

If the auditor is allowed to record without confrontation by security or police, the target is deemed to have passed the audit. However, if someone attempts to interrupt or stop the recording, the auditor will typically defend their position and argue their case, citing their legal rights; in this instance the target is deemed to have failed the audit.

Auditors typically post their recordings on social media to raise awareness of their activities, however this poses a threat of hostile reconnaissance (first or indeed second hand through viewing the recording) for target organisations, and negative brand and reputation impact.

Advisory

Managing the risks posed by security auditors comes with its own unique challenges. There are a number of specific actions organisations can take to safeguard against this threat, which can be aligned to the CPNI's principles of DETER, DETECT AND DELAY, MITIGATE and RESPOND, and its guidance on hostile reconnaissance.

- **DETER** stop or displace the attack.
- **DETECT:** verify an attack, initiate the response.
- **DELAY:** prevent the attack from reaching the asset (including measures to minimise the consequences of an attack).
- **MITIGATE:** minimise the consequences of an attack against your site.
- **RESPOND:** actions to prevent the goal of the attack being completed.

A comprehensive security strategy is key to managing any security threat and associated risk(s). There are additional strategies organisations can apply to counter the threat of auditing, and it should be noted that some strategies function more effectively at different stages of the auditing process.

- Raise awareness of the threat through ongoing training and education. Awareness of threat indicators is key; identifying early warning indicators could minimise the risk of any security incident, including auditing, being successful.
- For general awareness (and prior to the start of the auditing process) it is advised that organisations actively share visual guidelines demarcating public versus private spaces concerning the organisation's site. This could help avoid unnecessary altercations between auditors and security / members of staff.
- Organisations should provide security / members of staff with information surrounding laws concerned with recording from a public space.
- Perform a dynamic risk assessment if an auditor is identified in operation:
    - Is the individual or group displaying signs of the auditing movement? What is the intention?
    - What is the risk to the organisation or employees?
    - Could the site be targeted by criminals? Why?
    - Is the site in a high footfall area?
    - What is the intent of the individual / group?

- Once an auditor has begun recording and initiated an interaction with security / member of staff, it is advised:
    - To remain calm and polite.
    - To not engage with the auditor’s remarks and questions any more than necessary.
    - Avoid engaging in ‘debate’ with the auditor.
    - To not physically hinder the auditor’s recording process.
    - To not provide an emotional or physical reaction to attempts at provocation from the auditor.
- Security personnel and employees can be empowered to identify suspicious activity and how to manage this by completing See, Check and Notify (SCaN) training. SCaN enables employees to effectively assess the risk posed by individuals or groups who seek to gain information to cause harm to an organisation or individual.
- **If there are genuine concerns the recording is for the purposes of crime or terrorism, inform police immediately.**

Intelligence assessment

The SIU assesses with HIGH CONFIDENCE that the security auditing will increase due to its growing popularity as an effective and relatively straightforward means of promoting rights and freedoms, and holding governments and organisations to account. Any determined individual is capable of auditing with access to basic recording equipment and a grasp of laws and regulations concerning filming in public spaces.

While public organisations and operations make up the majority of current targets for security auditors, it is likely that this will expand across industries and sectors. This could be linked to COVID-19, such as organisations imposing restrictions in the workplace (i.e. mandatory use of face coverings, social distancing vaccines etc. above and beyond government guidance and official requirements), or other factors, including perceived business faults, such as corruption, unethical business practices and climate change. Ultimately, as with all forms of protest related activity, any organisation could be targeted by specific groups / individuals, utilising auditor TTPs.

The most likely course of action (MLCOA) related to a security auditor event, is a challenging engagement between the auditor and security, with the accompanying footage posted online, resulting in brand and reputational impact.

However, the most dangerous course of action (MDCOA) is that the security auditor is undertaking hostile reconnaissance for a protest, criminal, or in the worst case, terrorist act. Any one of these could result in disruption to operations, damage, and threat to health and safety, and ultimately life.

In relation to protest activity auditing shares some aspects with non-violent direct action (NVDA) strategies adopted by Extinction Rebellion (XR) and used prominently and effectively in past campaigns. NVDA is a strategy that enables activists to cause severe levels of disruption without breaking the law or giving police justification for arrest. The success of NVDA relies on the individual engaging in the action understanding the laws surrounding protesting and acting within the ‘letter of the law’, much like auditing. Because of the similar tactics and requirements, it cannot be ruled out that activist groups could adopt auditing as part of their NVDA strategy and use it as a tactic to pressure private businesses or bodies that they have deemed ‘viable targets’.

Additionally, TTPs used by security auditors have been observed during demonstrations to film the response of the police during recent events (Kill the Bill, Black Lives Matter etc). The use of similar tactics at protests targeting organisations cannot be ruled out.

The threat posed by security auditors serves to highlight **just one determined individual can cause significant disruption** and businesses should take proactive measures to manage this risk.

Intelligence Cut Off Date (ICOD):	2359hrs, 16 May 2021.