DAWN RAID THREAT

It's something nobody expects and in all likelihood is not planned for. Yet the number of early morning raids by authorities on media companies is rising. Here's some useful advice

Picture the scene: Everyone is in Cannes for MIPTV, the international TV and digital content market. After a night of sipping champagne, celebrating success and exchanging news and gossip you're jolted awake by your phone ringing. A panicked junior team member, one of the few left in your office to hold the fort, tells you that European Commission (EC) officials have arrived at 8 am and begun raiding your company, seizing laptops, hard drives and mobiles.

Apparently, they're looking for suspected anticompetitive agreements. You tell the person on the phone not to panic, but what do you do? What can you do? What is the exposure?

NO FICTION

This is not a hypothetical scenario. This April four broadcast industry companies found themselves subject to so-called 'dawn raids' by the EC officials over suspected participation in a sports rights cartel. Such dawn raids are on the rise across Europe, with competition authorities increasingly willing to obtain information in this way. They like dawn raids because they nearly always achieve total surprise. It's very rare that a company has a suspicion that it might be raided, and in the cases where a cartel actually does exist, often very few people will be aware of the fact.

> "Dawn raids are real. This April, four major broadcast companies were targetted by EC officials"

DISRUPTIVE AND DISTURBING

The effect of dawn raids on companies ranges from extremely disruptive to absolutely terrifying. If the raid happens in Europe, officials have the right to enter business premises – and sometimes private homes – to take away hard and soft copies of documents and other information relating to a suspected anticompetitive agreement, such as a membership of a cartel, bid rigging or price fixing. They can also interview individuals. In the EU, failure to cooperate can either increase the ultimate fine or be treated a separate offence, which also

carries a fine.

In the US, the equivalent of an EC dawn raid is the execution of a search warrant, one of several options the Department of Justice can use to gather evidence of hard core competition law (or antitrust, as it's called in the US) violations. While cartels, price fixing and bid rigging are mostly non-criminal offences in Europe, they are crimes under US law. As a result, search warrants in the US will often be executed by armed law enforcement officers.

The arrival of armed FBI agents in reception can make a US dawn raid particularly intimidating, but US employees are at least likely to be familiar with the concept of a search warrant and to take the situation very seriously. This doesn't always happen in the EU; it's not uncommon for security guards to think the EC officials are part of a hoax and to ask them to leave. Doing so is an offence in both Europe and the US. Companies and their employees must not obstruct the agents conducting a search.

Whether in Europe or the US, dawn raids present similar risks, and best practices for handling dawn raids are very similar on both sides of the Atlantic. The first half-hour of any such unannounced inspection is critical and how you handle this, or how you train your staff to handle it in the event of your absence, can have a significant influence on how the investigation unfolds. It's crucial to train and put in place practices that help staff with such a disruptive and upsetting experience.

CONTINGENCY MEASURES

Security and reception should be trained to ask dawn-raiding agents to wait until the lawyers, or at least the senior executives, arrive. Reception should make the agents comfortable and try to move them into a separate waiting room or holding area until the house lawyers are there. However, it's important that security knows not to obstruct them if they refuse to wait, as they're not required to do so. Reception should, however, record the agents' names and information from their official IDs, and request business cards. They should also ask for a copy of the warrant, or the decision authorising the inspection.

▲ Cannes by night, where there are many, many parties for MIPTV participants

Reception should immediately call both the company's counsel and external law firm, and email them copies of the warrant, authorisation and any other documents. Some law firms may offer a 'dawn raid hotline' whose number can be pinned behind reception, together with a short 'dawn raid to do list'.

Once a senior person arrives, they have the right to cross-check whether all of the raid team are mentioned in the decision document. If they're not, identify which ones are missing and tell the lawyers. Also note, for the benefit of the lawyers, whether the search warrant correctly identifies the address being searched. In addition, inform the agents that the head of legal (or his/her designee) is the only person on site authorized to speak for the company regarding this search. In the US, if asked, other employees should say that they are not authorized to consent to the search of any company property or records, but that they intend to cooperate. Above all, no one should attempt to obstruct the agents' access to areas they intend to search.

MITIGATING IMPACT

It is key to have in place an internal response team – including security, reception and IT – that has been trained in how to handle such investigations and how to cover the period from the arrival of the agents until the arrival of the external support team. You will also need to have in place a general communications plan and to ensure that it is aligned with and can draw upon your wider crisis management team and plan.

During the dawn raid, the main focus will be on ensuring that the inspection runs as smoothly and quickly as possible while at the same time safeguarding the company's (and potentially individuals') rights of defence. Often this is done in a vacuum, as the company is unlikely to be aware of the allegations that are being investigated. In parallel, senior management will want to understand what is happening, but must avoid destroying evidence and tipping off other companies who may be at risk of a raid.

Having these procedures and training in place will help avoid some nightmare scenarios. For example, in one European raid, the officials asked a Czech energy company to block certain email accounts. During the inspection, the officials discovered that instead of fully blocking the account, the company had diverted all new emails from that account to a different account. The company was fined EUR2.5m for obstructing ▶

the raid.

The authorities and state officials may adopt different approaches in the EU and the US, and trans-Atlantic companies will need to be sensitive to this. For example, in the US, law enforcement agents executing a search warrant are more likely to take a broad brush approach, gathering (or copying) all potentially relevant files, computers and storage media as quickly and efficiently as possible, rather than waiting in a holding area and taking 2-3 days to sift through physical or electronic documents individually, as is common in Europe. In Europe, national competition authorities all have their own approaches to raids, and even the EC's raids differ somewhat between case teams and over time.

KEEPING CALM

While you can't plan for all eventualities, showing that you are not panicking and have general procedures in place will greatly encourage the raiders to respond positively, or at least lower the temperature of the initial phase of the raid.

Where an inspection takes more than a day (and in the EU most do take multiple days), filing cabinets or entire rooms will be sealed overnight. In one case where a German company broke such a seal, the European Commission fined it EUR38m just for interfering with the investigation (even though this was unintentional).

The IT team is crucial in any dawn raid. The investigators will need to review electronic documents, emails and other electronic comms. The IT team will need to work with the investigators to secure the data, and to ensure the company keeps a copy of what the investigators searched or copied.

It may have been the case for those broadcast companies that were dawn-raided during MIPTV that the in-house legal team were out of the office. Whether or not they are, a team of external lawyers needs to come in quickly. You'll need a lot of lawyers on the ground, ideally one to shadow each member of the dawn raid team. The lawyers need to ensure that, if at all possible, the inspectors only take documents to which they are entitled, and try to build a picture of the likely focus of any ensuing investigation.

Dawn raids are inherently stressful situations, and each one has different pressure points and sensitivities to overcome. Simply having one's laptop and phone taken away for two hours and looked at is enough to send most people's adrenalin through the roof. Raids are also massively disruptive, and can all but shut down the unit under investigation for days, with people unable to work or indeed access their email.

Though we would not expect that the on air/production team at a broadcaster would be the target of a raid, in the high-octane environment of a news organisation, any such disruption will have a ripple effect throughout the company. As a broadcaster you will be acutely aware that such raids attract significant press interest, which means that you will need to think about your own communication plan and strategy, which will need to fit within your wider crisis management response plan.

▲ Definitely do not delete files on computers or destroy paper documents

> "Showing you are not panicking and have procedures in place will help the raiders to respond positively"

John Schmidt and **Wilson Mudge** are partners in, respectively, the London and Washington, DC offices of law firm **Arnold & Porter**.