A typical dawn raid day

09:00 hrs: officials at the door

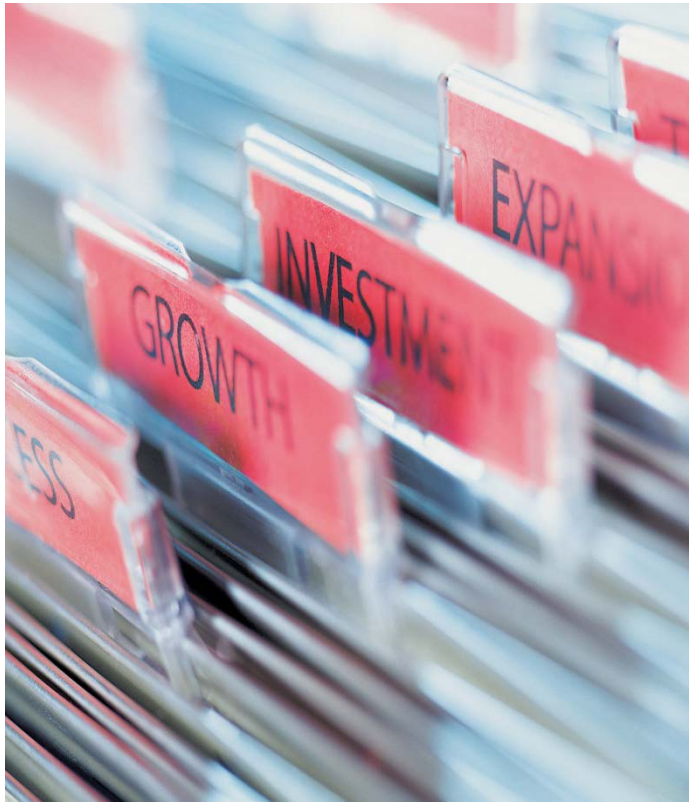
09:45 hrs: arrival attorney

10:00 hrs: start of analogue and digital inspection

14:00 hrs: interview employees

18:00 hrs: end inspection / affixing seals

18:20 hrs: de-briefing and next steps



DE BRAUW
BLACKSTONE
WESTBROEK

09:00 hrs: officials at the door

- Reception:

- Identification check:
  - Check valid ID cards
  - Copy ID cards
  - Ask for the objectives of raid
  - Ask for a written document indicating the objectives

  - **Note**: *inspectors must identify themselves and clarify the objective of the raid, but a written document is not always required.*

Key actions:

- Remain calm, polite and cooperative
- The first hour is vital

09:00 hrs: officials at the door

- Reception:
- Contact the Raid Coordinator
- Invite the inspectors to kindly wait in a private meeting room.
  - Do not let the inspectors wait in a public area of the building.
  - Ensure that the inspectors are escorted at all times.

Key actions:

- Get organised
- Assemble team: Raid Coordinator, ICT specialist, document managers and external counsel.
- Requests the officials to wait for the arrival of external counsel.
- Do not answer questions until the Raid Coordinator has arrived.

Officials usually wait 30 min. Do not obstruct the inspection, if they do not want to wait any longer.

High penalties for non-cooperation.

09:00 hrs: officials at the door

- Raid Coordinator

  - Shares initial information with external counsel
  - Instructs ICT specialist
  - Instructs Document Managers
  - Contacts facility services
  - Contacts external communications: prepare holding statement

Key actions:

The Raid Coordinator:

- Maintains a good working relationship with the inspectors
- Involves external counsel in case of risk of escallation
- Facilitates an orderly raid and protects the company's rights and legitimate interests

09:45 hrs: arrival attorney / kick-off meeting

- The following should be discussed:

  - start investigation
  - timing
  - work procedure
  - search procedure
  - interview
  - confidential / privileged information
  - escorts of officials
  - IT back up
  - structure company business and premises
  - publicity

09:45 hrs: arrival attorney / kick-off meeting

- Ask the inspectors for clarification on the following:

  - The focus: what are the suspicions?
  - The scope: time period, individuals, etc.
  - Company's status: suspect/target, witness?
  - Which information are they looking for?
  - How can the company assist?

10:00 hrs: start of inspection

- Criminal law authorities:
  - FIOD, police,
  - OM,
  - examining judge
- Power to
  - search and
  - seize documents & digital information
- Except:
  - privileged documents

Action Company:

- Escort inspectors
- Keep record of all discussions with officials
- Make a list of
  - all files studied by officials (incl. location)
  - all copied / scanned documents (incl. location)
  - all objects seized
- Note all questions asked by officals and answers given

10:00 hrs: start of inspection

- Administrative authorities:
  - European Commission, ACM (competition)
  - DNB, AFM (finance)
  - CBP (privacy)

- Power to
  - examine business records and company books
  - digital and hard-copy

- Except:
  - personal documents
  - privileged documents
  - documents outside the scope of the inspection.
  - No “fishing expedition”

Action Company:

- Escort inspectors
- Keep record of all discussions with officials
- Make three copies of each document scanned /copied by officials
- Make a list of
  - all files studied by officials (incl. location)
  - all copied / scanned documents (incl. location)
- Note all questions asked by officals and answers given

10:00 hrs: digital investigation (i)

- Digital investigation:

  - documents inside / outside scope
  - personal / privileged documents
  - in case of outsourcing: assistance of service provider

IN BRIEF

MLex Summary: The European Commission has fined two Czech energy companies 2.5 million euros for obstructing unannounced antitrust inspections in November 2009. The companies were fined for failing to block an email account, which would have ensured officials' access to all messages.

ECJ recommends allowing access to global documents in dawn raids

Tuesday, 8 April 2014 (7 hours ago)

Henry Vane

The European Commission was justified in inspecting non-European documents in its dawn raid of power cable cartellist Nexans, an Advocate General (AG) of the European Court of Justice says in an official opinion.

10:00 hrs: digital investigation (ii)

- Officials can examine computer files:
  - passwords have to be provided
  - access codes need to be given for data stored elsewhere (parallel Dutch Supreme Court ruling)

> 3.9.10 Indien tijdens de tenuitvoerlegging van het beslagverlof echter redelijke gronden blijken te bestaan om te vermoeden dat de beslagene of de derde digitale bestanden elders dan op een aangetroffen gegevensdrager (bijvoorbeeld ' *in the cloud* ') bewaart, en dat deze bestanden vallen onder het beslagverlof, dient hij – onverminderd hetgeen hiervoor in 3.3.2 is vermeld - deze bestanden voor de deurwaarder toegankelijk te maken. De rechterlijke toestemming tot beslaglegging omvat in dit soort gevallen immers uit haar aard mede een tot de beslagene of de derde gericht bevel om de noodzakelijke medewerking te verlenen aan de beslaglegging omdat die toestemming anders zinloos zou zijn.

  - accounts can be blocked
  - IT experts will make a copy (“image”) of hard disk including removed files
  - inspectors will use search terms to find relevant data; company’s involvement differs

10:00 hrs: digital investigation (iii)

Action company:

- Have IT stand-by
- In case of outsourcing: inform service provider
- Inform employees whose computer files / mail accounts will be blocked
- Inform all relevant persons able to block and deblock accounts
- Provide hardware (DVD, connection cables)
- Make three copies of all copied files on DVD; this is not always possible with criminal law authorities
- Register all actions taken by officials

10:00 hrs: privileged information

- Handle privileged information with extra care:

  - In general the inspectors are not authorised to copy or seize information that is protected by privilege.
  - Identify to the extent possible all privileged information.
  - Request the inspectors not to copy or seize privileged information.
  - In case of unresolved discussions: request that the relevant information is sealed.
  - Take record of discussions.
  - To the extent possible, information containing commercially sensitive information should be marked as confidential.

14:00 hrs: questions & interview

- Practical questions to facilitate the raid should generally be answered.
- Refusing to answer a factual or procedural question, or giving misleading or incomplete answers, may be viewed as a violation of the company's duty to cooperate in the investigation.

Action company:

- Cooperate
- Never mislead

14:00 hrs: interview

- Employees can be interviewed

  - Criminal law authorities and European Commission: **voluntary basis**

  - right to an attorney
  - right to remain silent
  - incriminating vs factual questions

  - Advisable to tape interview?

Action company:

- Ensure presence of attorney

14:00 hrs: interview

- Prepare each interviewee to:
  - Listen carefully and tell the truth
  - Ask for clarification
  - Give clear and succinct answers
  - Answer only from personal knowledge
  - Not guess or speculate
  - Avoid giving conclusions or opinions
  - Not disclose privileged information
  - Consider the right against self-incrimination
  - Only sign minutes when they properly reflect your statements

Action company:

- Support and provide guidance to employees being interviewed

18:00 hrs: end of inspection

- Closing meeting
  - Identify data collected
  - Discuss unresolved issues
  - Discuss follow-up action such as
    - Agree on completion of collection
    - Agree on document preservation
    - Ensure e-mail account blocks
    - If rooms were sealed, ensure that the room remains sealed and guarded at all times

18:20 hrs: de-briefing and next steps (i)

- De-briefing with company personnel involved in dawn raid

  - Review the data seized / scanned / copied by the officials
  - In case of seals: inform cleaning / security staff
  - Find smoking gun
    - interviews
    - examining digital and analogue documents
  - In case of violation:
    - end violation
    - leniency?

18:20 hrs: de-briefing and next steps (ii)

- Subsequent reporting, communication and disclosure:

  - Provide report to management and the general counsel.
  - Consider whether further (internal) reporting is required, for instance to (internal) auditors, compliance, supervisory board, audit committee, or regulators.
  - Consider whether a public disclosure is required.
  - Consider whether document retention notices should be sent.

QUESTIONS?