Are you prepared for a regulatory raid?

Globally 'dawn raids' by regulators are becoming increasingly common on corporate organisations in relation to both civil and criminal matters. You may only become aware that your organisation and/or the employees in it are being investigated when the regulator arrives at your premises for a 'dawn raid'. Organisations need to have a clear set of procedures for employees to follow in the event of a regulatory raid – the reality is you won't have time to come up with a strategy on the day.

If you are unprepared for a regulatory raid, the risks include:

- inability to contact and bring together a response team quickly to deal with the raid;
- removal of documents outside the scope of a warrant, particularly when dealing with large volumes of documents, including electronic documents;
- claims for legal professional privilege are not made and/or waived;
- penalties (civil and/or criminal) for obstructing an investigation and/or concealing or destroying documents;
- inadequate management of communications adversely impacting the reputation of the organisation.

Who can raid?

There are a number of organisations that can exercise search and seizure warrants. Most in-house lawyers would be aware that the Australian Competition and Consumer Commission (ACCC) has powers to enter and search premises where it believes there may be material relevant to a contravention of the *Competition and Consumer Act 2010*.

The Australian Crime Commission (ACC), the Australian Federal Police (AFP) and the Australian Securities and Investment Commission (ASIC) also have wide-ranging powers to enter and search premises, compel the production of information and seize records for the purpose of investigating suspected breaches of the law. These powers have expanded over the years, particularly in response to serious corporate misconduct and white-collar crime.

Project Wickenby is an example of a cross-agency task force (one which includes eight federal agencies) dedicated to fighting tax evasion, avoidance and crime. As the ATO website explains, this task force also works with governments and organisations around the world to fight tax evasion and avoidance on a global scale. Since it was established in 2006, it has involved:

- criminal investigations conducted by the ACC, the AFP and ASIC; and
- administrative actions, including audits, banning people from the financial services industry and using data from the Australian Transaction Reports and Analysis Centre (AUSTRAC) to track money moving in and out of Australia.

CHECKLIST FOR HANDLING A REGULATORY RAID

Develop Regulatory Raid Plan

Preparing a 'Regulatory Raid Plan' appropriate to your organisation will assist in establishing the regulatory raid response team as well as ensuring periodic meeting and training of the team. It will also serve as a guide to remind the team of their roles in the event of a regulatory raid.

Establish response team

Prepare a list of employees who will make up the response team in the event of a regulatory raid. This will include: a regulatory raid manager (senior lawyer/manager with responsibility for overall management of the response), in-house lawyer(s), senior IT personnel, senior communications manager, and other employees who will observe or shadow each of the investigatory teams as a search is carried out. The list should contain full contact details of key internal staff members and the contact details for your external law firm, including mobile numbers.

Train team members

The dedicated response team should meet periodically and receive training so that all members of the team understand their roles and responsibilities. Training should ensure that employee observers understand their roles, which will include: making copies of documents that are seized; taking notes of questions and answers provided during the course of the search; and checking that documents seized are within the scope of the warrant. Training should also include a review of the data retention system for both hard-copy and electronic documents, provide a practical understanding of the difficulties presented by searching and producing documents, and explain how to make claims for legal professional privilege.

During the raid

- ***Investigators' arrival***
  The investigators may request to see specific personnel. Ask the investigators to wait in a meeting room until any personnel they have requested to see arrive and a senior in-house lawyer is present. If the investigators refuse to wait, permit them to enter but make a note that they refused to wait.
- ***Call response team immediately***
  It is critical that as many of the response team as possible are able to convene as quickly as possible, so they are able to observe the investigators from the outset as they proceed to search and seize documents. The regulatory raid manager should provide each of the response team members with the 'regulatory raid procedure' document to remind them of their role on the day.

- ***Check identity cards***
  Ask to see the investigators' identity cards. Either make a note of the name and title of the officers or make copies of the cards. Ensure that you have the mobile number of the lead responsible officer so that you can contact that officer directly.

- ***Check warrant***
  You need to read the scope of the warrant and any other documentation, understand the type of evidential material the subject of the search, and check that the search is being carried out within the time frame allowed by the warrant. Take your time to fully understand the documents and make a copy of the warrant and any other documents shown to you by the investigators.

- ***Observe search***
  Do not leave investigators alone while they are on the premises. A lawyer(s) and/or appropriate employee should be present, observing and shadowing each of the investigatory teams at all times. Other matters to consider include:
  - Clearly identify the contact persons if any of the observers have questions: allocate a senior member of the IT team to assist with IT-related queries and a senior in-house lawyer to deal with privilege or other legal issues that may arise.
  - Where IT forensic officers are involved in the search and seizure of documents, it is particularly important that employee observers understand and are competent to deal with electronic documents and IT systems.
  - You may wish to make a video recording of the search.

- ***Inform staff***
  Inform staff of the nature of the investigation, instruct them to co-operate with the investigators, and make them aware that documents must not be concealed or destroyed. Ensure that employees are aware that third parties must not be told about the investigation. Provide the name and contact details of the in-house lawyer for any questions.

- ***Seizure of documents***
  Ensure that documents being seized fall within the scope of the warrant. Any document the investigators seize should be copied and those copies should remain with the company. Where electronic data is taken or hard drives removed, copies should be made.

- ***Documents in dispute***
  Try to agree upon a process for documents that are in dispute, such as placing them in a sealed envelope, to be held by a third party.

- ***Make privilege claims***
  Ensure that claims for legal professional privilege are made over documents where claims are justified. You may need to briefly explain why you consider the document privileged from production, for example, by saying that the document was prepared by a lawyer and/or showing the part of the document with the sign-off showing a legal title. Documents subject to legal professional privilege should be identified and

placed in a sealed envelope, to be held by a third party. Unless the claims for privilege are accepted, you will need to commence proceedings promptly to establish privilege.

- ***Answering questions***
  When answering officials' questions, be honest, brief and to the point. Keep a record of the questions and your answers. In general, investigators can ask where a document can be located and for an explanation of the document within the scope of the warrant. Where possible, any information or statement regarding the facts of the subject of the investigation should only be made in the presence of a lawyer.
- ***External communications***
  Prepare a low-key press release to be issued when news of the raid leaks or an announcement is made. If you are a publicly listed company, consider whether you are required to make any notifications to regulators including the Australian Stock Exchange.

For further information, including tailored regulatory raid plans and training for your organisation, contact Susan Bennett, Principal +61 2 8226 8682 or email susan.bennett@sibenco.com.

This article is for reference purposes only and does not constitute legal advice.