## Dawn Raids – Top 10 Tips

### Before

1. **Get your House in Order**
   
   Know where your data is: create a data inventory or a data map. Ensure compliance with a company backup policy and securely destroy old data outside of that policy. Keep individual data access to a minimum. Conduct internal audits to uncover potential breaches. Regulators can fine for poor access controls so ensure suitable encryption exists. Consider the implications of using personal devices.

2. **Be Prepared**
   
   Attend training or conduct a mock dawn-raid to test the effectiveness of compliance procedures and understanding within the company. Have you created Dawn Raid procedures and assigned a response team?

3. **Inform Management, Lawyers & Advisers**
   
   Be welcoming and polite to Investigators and, if possible, wait for the lawyers to arrive to check and understand the warrant or search order. Depending on the nature of the enquiries being made and the type of warrant there may be nothing to stop the investigators proceeding immediately. Consider enlisting the help and advice of a forensic technology consultant to shadow the Investigators. Handle communications within the firm to ensure there is understanding and compliance with the Investigation and that your reputation is protected.

### During

4. **Know your IT Administrators**
   
   Get your IT people involved early in order to grant access to electronic data and individual custodians. Investigators might require Internet access, LAN access and USB access to install and run their forensic imaging software. Make sure that the tools they are installing, if any, are forensically sound and virus free. Passwords may also be required for any encrypted hardware, software, folders or documents.

5. **Co-operate**
   
   Ensure all members of the company are aware of the legal obligation. Do not turn off computers as Investigators might request access to Random Access Memory (containing passwords, clipboard content etc.) which would disappear upon loss of power. Protect any seals (e.g. tamper proof evidence bags, locks on doors) left by the Investigators or risk hefty fines. Do not delete data – deleting data can leave a trace and lead to uncomfortable enquiries.
6. Negotiate

Business continuity is important. Is it necessary for whole computers to be seized or for servers to be taken off-line? Highlight individual areas of potential relevance and consider approaches to ensure known privileged documents are not seen by Investigators. Procedures may be agreed to seize disputed documents to be sealed for a review by an independent lawyer to determine privilege.

7. Take Copies

Take copies of everything seized, copied or seen by Investigators. This may or may not be possible during the course of the execution of the warrant. As a rule Investigators are obliged to provide a list of seized items but not copies. A forensic technology consultant will be able to assist by using forensic software to ensure that source data is not altered in any way and that crucial metadata remains intact.

8. Monitor

Have the Investigators taken adequate steps in securing the data to ensure data protection and data integrity? Are they taking documents outside the scope of the Investigation or documents with privileged information? Are they using suitable software, tamper proof evidence bags and maintaining chain of custody? Are they creating an inventory of recoveries, clearly labelling data and avoiding cross-contamination? One of the most important things during the course of a raid is to take copious notes of what they are searching for and on which machines.

9. Stay Ahead

If sufficient notes are made during the course of the search then it is often possible for a forensic company to reconstruct what has been searched. Consider a further internal audit, in order to preserve more data than the regulator, which might strengthen your case. Refer to the ‘Electronic Documents Questionnaire’ (referenced in the UK Civil Procedure Rules – PD 31B) to assist in your search for relevant documents.

10. Review

Use a legal technology provider to setup an Early Case Assessment of all the documents seized by the regulator plus any further documents identified. Filter and prioritise documents for review using the latest technology to quickly prepare your response.

Why Kroll Ontrack?

With the most comprehensive line of electronic evidence services in Europe, Kroll Ontrack can design tailor-made electronic evidence solutions just for you.

Our consultants have years of experience working with forensic specialists, regulatory bodies and government organisations including the SFO, HM Customs & Excise, FSA, United States Air force and the MoD.