# Monitoring and response

JANET(UK) recommends that organisations connected to JANET carry out their own internal monitoring of their network connection. On a simple level the JANET Netsight system can highlight abnormal traffic levels on a site's access link that may be a result of illegal activity. The JANET Factsheet Unusual Traffic [1] gives examples of how Netsight can be used to detect these kinds of problems.

JANET(UK) also recommends that organisations record sufficient information about the use of their networks and maintain tools which enable them to investigate and deal with problems. Note that any logging or monitoring that results in data about individual users will be subject to the Data Protection Act 1998, while any actions that reveal the content of communications are subject to the Regulation of Investigatory Powers Act 2000. Such actions must be properly authorised, controlled and notified to users, or else they may be criminal offences.

- The Data Protection Act 1998 can be found at: http://www.hmso.gov.uk/acts/acts1998/19980029.htm [2]
- The Regulation of Investigatory Powers Act 2000 can be found at: http://www.hmso.gov.uk/acts/acts2000/20000023.htm [3]
- The Employment Practices Data Protection Code Part 3: Monitoring at Work issued by the Information Commissioner deals with both logging and interception. It is available from: http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/codes_of_practice.aspx [4]
- The JANET Technical Guide Logfiles [5] discusses the legal and technical issues involved in the recording of usage information.

Active monitoring of networks can be used to obtain more detailed information. This can range from scanning networks to identify the machines present and the services they run, to full penetration testing using all the tools of intruders (technical and social) to assess the preparedness of a network and its defences. Such activities should be carefully planned with clear objectives, or a great deal of time, effort and money can be wasted. In addition to the laws mentioned above, active monitoring is also likely to be subject to other legislation including the Computer Misuse Act 1990. Monitoring must only be done with the appropriate authority on networks and systems that the organisation controls.

JANET CSIRT [6] is able to provide advice on monitoring tools for all sites. FE and specialist colleges may also be able to receive assistance from their JISC RSC.

Detecting security problems will have little effect unless the organisation also has processes, tools and skills available to investigate and remedy the problem. The JANET Guidance Note on Effective Incident Response [7] contains practical ideas and case studies on how this can be done at JANET sites.

**Links**

[1] http://community.ja.net/library/janet-services-documentation/unusual-traffic%20
[2] http://www.hmso.gov.uk/acts/acts1998/19980029.htm
[3] http://www.hmso.gov.uk/acts/acts2000/20000023.htm
[4] http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/codes_of_practice.aspx
[5] http://community.ja.net/library/janet-services-documentation/logfiles-technical-guide
[6] http://community.ja.net/library/janet-services-documentation/janet-csirt
[7] http://community.ja.net/library/janet-services-documentation/effective-incident-response