Methods of countering the threats

There are two main technical approaches that an organisation can use to address security issues

- Computer Security: secure configuration, operation and maintenance of computer systems
- Network Security: implementation of security measures at routers, firewalls and other network control devices, both within the LAN and at the organisation's perimeter connection(s) to Janet and the Internet

Communications security, for example ensuring that sensitive information is encrypted when it passes over networks, involves both computers and networks.

All of these must be supported by non-technical measures, such as policies and user education, since deliberate, careless or reckless behaviour by users can defeat any technical security measure.

It is likely that most organisations will need to use a balanced combination of approaches, including applying stronger network security measures to areas where computer security is more difficult to achieve or where computers or information are subject to increased risks.The ideal would be to ensure that every computer was secure in every aspect of its use, since this has benefits for all other computers and users on the network. Only computer security can be effective against internal attackers and external attackers who have managed to compromise an internal computer or user account as a bridgehead. Unfortunately perfect computer security is impossible to attain - particularly since the organisation is unlikely to control all the devices that may connect to its network - so network security will always be required as an additional precaution.

Network security can also be used to partition the local network into zones where different security conditions apply, for example zones might be used to separate:

- systems that are at high risk because of the value of their information or service;
- centrally managed workstations;
- other client computers (e.g. visitor or personal devices that the organisation does not manage);
- administrative systems.

The network security approach is useful both within and at the boundaries of the organisation’s network. In particular, using appropriate controls at the network level can limit the spread of future incidents as well as allowing effort to be concentrated on securing the small number of hosts which, to carry out their function, have to be most exposed to possible attack.

Recent developments, such as cloud computing and Bring Your Own Device (BYOD), may alter the boundaries between networks and domains of control over computers. With cloud computing, sensitive data may be stored on virtual servers in data centres where the organisation does not control the network. BYOD means that organisations can no longer impose device configurations but need to agree them with their owners. These, and other, developments make it even more important to adopt a holistic approach to security, using technical measures on computers and networks and behavioural policies followed by users, to achieve the security that the organisation requires.

Section 3, Computer Security [1] deals with some issues of securing computers. Some practical advice is given, although this has been kept brief as there are now many detailed guides available to assist. Details of where to obtain such material, much of which is in the public domain, are given in Related information [2]. It cannot be emphasised too strongly how important it is that an organisation connected, or planning to connect, to Janet ensures that it regularly checks its own security in the light of the practical recommendations made in these or other documents.

Section 4, Network Security [3] deals with security implemented via the organisation's network control devices, both within the organisation and at its Janet connection. It covers the advantages and disadvantages of security measures that use network devices, and some practical considerations that may arise.

Finally, it should be remembered that, although this guide deals only with the technical aspects of the provision of security, there are other considerations, both administrative and legal, that need to be taken into account. Indeed, there is little point in devising technical solutions to security threats if there is no organisational information security policy, supported by senior management, supporting the measures to be implemented. This policy should set out clearly the responsibilities and authorities of all users and providers of the service to protect the security of the organisation and its information: the interconnected nature of an IP network means that insecure behaviour by one user can cause significant and widespread damage to others. In formulating a security policy, items that need to be addressed include establishing acceptable behaviour rules for members of the organisation, enabling them to use computers in a secure way and defining procedures to be followed when violations of security are detected. Those developing their own policies and rules may find UCISA's Information Security Toolkit [4] and Model Regulations [5] helpful. References to these and other sources of information about security policies are given in Related information [2].

Links
[1] http://community.ja.net/library/janet-services-documentation/host-security
[2] http://community.ja.net/library/janet-services-documentation/related-information
[3] http://community.ja.net/library/janet-services-documentation/network-security
[4] http://www.ucisa.ac.uk/publications/toolkit.aspx
[5] http://www.ucisa.ac.uk/publications/modelregs.aspx