Reasons for incident response

There are a number of different reasons why a Janet customer site should improve its response to computer security incidents. Depending on the circumstances, different reasons will carry different weight in each organisation: however an effective incident response function should bring benefits in all these areas.

All Janet sites should already have some form of incident response, as this is a requirement of the policies that govern connection to the network. The Janet Security Policy [1] requires in section 16 that every site behave responsibly by 'assisting in the investigation of a breach of security' and in section 12 that they 'identify individual points of contact … available to provide and receive information on behalf of the organisation'. Sites that provide connection to others under the sponsored or proxy licensing schemes must also satisfy these requirements on their behalf. All sites must therefore notify Janet of a Security Contact who can disseminate security-related information within the organisation and help to resolve any problems that arise. Security Contacts are not necessarily expected to fix security problems themselves, but must ensure that the necessary action is taken by the organisation and act as liaison with Janet-CERT until the problem is resolved.

The main purpose of the Janet Security Policy is to protect Janet and to ensure that the actions of individual sites do not disrupt the service provided to others by the network. This requirement of the policy could be satisfied by simply disconnecting any computer or site about which there is a complaint. However such an approach is unlikely to be acceptable in the vast majority of Janet customer sites where computers and networks are essential for the daily operations of the organisation, whether in teaching, research or administration. An organisation that relies on computers and networks needs to identify and resolve problems quickly so that normal service can be resumed as soon as possible and disruption to staff and students is minimised. An incident response function, backed by policies and granted resources and authority by the organisation, can be a very effective way to achieve this essential business aim.

There are an increasing number of laws that require organisations running networks to respond promptly to requests. These range from data protection, through defamation to the protection of children. An organisation that does not respond promptly may find it has incurred civil or even criminal liability. An incident response function can help directly in many of these areas and can provide a contact point and support for requests in areas such as data protection and freedom of information that are likely to be the responsibilities of others in the organisation.

Responding promptly and effectively to reports of problems also raises the reputation of the organisation. Incidents such as web defacements, bulk mailings or Internet worms give a very public announcement that a site has security problems. Those who have seen their problem dealt with courteously and efficiently are likely to have a better opinion of those who helped them. The Janet network has an excellent reputation world wide, which gives many benefits

when we have to deal with other networks and with law enforcement agencies. In the same way, organisations that have a good reputation on the Internet are likely to find that others are, in turn, more willing to help them and that they have become part of a virtuous spiral that can make computer and networks more effective for us all.

Links
[1] https://community.ja.net/library/janet-services-documentation/reasons-incident-response