Effective incident response

GD/NOTE/009 (03/09)

Computer security incidents can be very disruptive for universities and colleges that rely on computers and networks for their work. Security incidents usually prevent computers and networks performing their intended function. If not resolved promptly, an incident can also cause problems for those who are likely to blame the organisation: at best this will damage their reputation but it may also have contract and legal implications. It is therefore very much in the organisation's interests to be able to respond promptly and effectively to computer security incidents.

In fact every connected organisation on the Janet network will already have someone who is performing at least basic incident response tasks, if only on an informal basis. The conditions of connection to the network require there to be a site Security Contact in order to protect the network. This Guidance Note explains how this basic incident response function can be developed gradually to provide more effective protection for the organisation's computers, networks and users.

The first stages of organising an effective incident response function are often possible using existing resources, supported by management through effective organisational policies, but to achieve the greatest effect is likely to need investment of time, people and equipment. Well-planned investment in incident response will result in a better computer and network service for the organisation. An organisation that responds promptly and effectively to incidents is also likely to find its reputation enhanced so that others will be quicker to help when it is the victim of incidents elsewhere.

The first section of the Guidance Note sets out the reasons why incident response is important to Janet customers. The different services that can be provided by, or in association with, an incident response function are then discussed, identifying three groups of services – basic, additional and extended – that have been found particularly useful in universities and colleges. People are essential to incident response, so there is then a section on different ways to arrange staffing of an incident response function. These include options for both full-time and part-time members of an incident response team: different models will suit different organisations but both can be very successful. There is also a discussion of the other skills that incident response staff may need to call on. To make this more concrete, three case studies describe how different Janet customers have arranged their incident response functions. To be effective, incident response must be supported by organisational policies, so the final section discusses these. Staff involved in incident response can often make useful contributions to policy development since they experience at first hand the problems that damage the organisation's computer and network services.

The Guide combines experience from Janet sites with that from other incident response groups in the UK and internationally. Thanks are due to those Janet sites that have contributed their experiences to the questionnaire and as case studies. Discussions with

national teams have also been very useful, especially the CERT (Computer Emergency Response Team) Co-ordination Center (CERT® /CC), whose Handbook and web site on CSIRT (Computer Security Incident Response Team) development have an immense amount of useful information for anyone building or enhancing their own incident response function.
