Incident response functions

From the preceding discussion it is clear that any organisation connected to Janet must have at least a basic response capability to deal with security incidents as required by its Janet contract. There are also good reasons why the organisation should not be content with this minimum but should provide additional functions for the benefit of its own users and its operation. This extended capability is likely to involve people and groups beyond the basic security incident response group, some of whom may be located in a different part of the management structure. However there are sufficient common features that sharing of at least information and experience, and possibly also staff and tools, should be of benefit. Any response function will inevitably receive some mis-directed requests, and co-ordination with other teams within the organisation is the best way to ensure these arrive at the right place to be dealt with promptly.

Whatever level of incident response is provided it must be authorised and supported by organisational policies that are respected by all users. Effective incident response requires prompt action to isolate and investigate the problem. If users do not recognise the authority of incident responders the necessary actions will be delayed and may even, in some circumstances, be illegal. The development of policies is discussed in Section 6 but needs to take place alongside planning of incident response functions and staffing, which are the topics of the next three sections.

Basic Security Incident Response Capability

To satisfy the Janet Security Policy every connected site must at least identify an e-mail and telephone contact point to receive and disseminate information and must be able to deal with situations where a problem system or user at the site is harming or threatening the network. These requirements define the minimum incident response capability that every site must provide.

Incident Handling

There must be a contact e-mail box and telephone, with a person or persons assigned to respond to these. Contact details for each site are maintained by Janet Customer Services (JCS), and sites are responsible for ensuring that their details are up to date. The Janet Security Policy does not state precisely what delay is acceptable in responding to messages sent to these, as this will vary from case to case. However Janet-CERT will take a view on the urgency of a response in any particular incident and, if a sufficiently rapid response is not received, will seek authority to temporarily remove a threat (possibly an entire organisation) from the network. To prevent this being done unnecessarily, a person who receives a message to the site contact point should confirm to the sender that the message has been received and that action is being taken to address the problem.

A site could, in fact, satisfy the requirements of the Security Policy by simply disconnecting

itself from Janet until each problem had been resolved. In practice this is unlikely to be acceptable to local users, so the Security Contact must have the tools and the authority to identify quickly the source of a problem within a site and to deal with it. Problems usually arise either from particular users or from a particular computer, so the basic requirement is to be able to understand the nature of the problem, identify the computer or user that is causing it and take action to prevent further damage, for example by disconnecting or blocking a computer's access to the network or by suspending the account of an individual user. This requires up to date records of computers, IP addresses and user accounts, and tools to search and combine these records. For key systems, and areas that are not under the direct control of the central computing service, lists of the responsible individuals will be needed so they can be contacted quickly when problems arise.

This containment action stops an incident causing continuing problems to external users, sites, or networks. The cause of the incident can then be investigated and resolved to remove the local disruption. In some cases a problem may be resolved sufficiently quickly that the initial containment stage is not needed, but the contact should be sure, if necessary confirming this with Janet-CERT, that this course of action is appropriate.

Alerts and Warnings

The Security Contact at each Janet connected organisation is also required to receive and disseminate security-related information within their organisation. Janet-CERT issues alerts and warnings of new threats to computers and networks and preventative measures that should be taken. Organisations are also encouraged to ensure that they receive security information distributed by the vendors of computer and network equipment they use.

Ensuring that this information reaches, and is acted upon by, all appropriate people within the organisation requires the same list of equipment needed for incident response, along with the contact details of the individuals responsible for that equipment. Various means can be used to forward information to these individuals: mailing lists and internal newsgroups or websites are common. These allow information about particular types of system to be distributed only to the groups that use them, but keeping such lists up to date can be a challenge.

Additional Security Functions

Most organisations will find that they need to add to the basic incident response capability described above to provide an effective computer service to their users and support the work of the organisation. The basic response capability is concerned with meeting external commitments, so provides little support to local users and system administrators. The first stages in enhancing this basic capability should be to support these users, both reactively after incidents occur and pro-actively to improve security awareness and preparedness to reduce the number of incidents suffered by the organisation.

Incident Response Co-ordination

While the basic incident response function merely eliminates problems, possibly by excluding users or systems from the network, an enhanced function should try to help local users and systems administrators to resolve problems and prevent them occurring again. This may involve hands-on technical help, for example to rebuild compromised systems. In the medium term, however, it may well be more effective to help users and administrators resolve their

own problems, rather than doing it for them. The role of the incident handler then moves from responding to the incident to co-ordinating the organisation's response: as well as helping the system administrator to find technical advice and tools it may also be necessary to work with the legal or public relations departments to help the organisation recover from the problem.

Announcements and Information Dissemination

The basic incident response function deals mainly with information that needs to be acted on immediately, whether this is concerned with problems at the site, new vulnerabilities in software or new forms of attack. However there is also a great deal of valuable information that can be used over the longer term to improve the security of the organisation's information and systems. As a response function grows, it should start to use its distribution channels to communicate this type of information to appropriate members of its internal constituency. Much of this information can be classified as good security practice, but this covers a wide range: for example, using protocols that encrypt login credentials rather than passing them over networks in clear text, configuring systems defensively rather than in the trusting mode still supplied by many vendors, or designing networks to reduce the likelihood and impact of a breach of security. A service that can disseminate this kind of information and promote its adoption within the organisation can greatly improve the security and stability of the networks it protects.

Awareness Building

In their early stages incident response teams tend to concentrate on technical problems, but many security issues can only, or most effectively, be solved by working with people. If users do not understand the need for technical security measures, whether they be passwords or firewalls, they will see them as inconveniences and use all their ingenuity to work around them. Building awareness among users of why security is important to them, and how they can help to support and promote it, can be a slow process but is the only way to achieve a genuine security culture. A security team should use all the means of communications available to it to promote its message: various teams have made effective use of training courses and short talks, articles in newsletters, posters, login banners and questionnaires. Informing and educating the user community will take time and persistence but can be highly effective.

Extended Services

Beyond these initial services there is a wide range of others a security team can offer to its community. Few, if any, teams offer all possible services: most choose the services where they can provide the greatest benefit to their user community. In the security incident response area, the CERT®/CC publishes an extensive list of services that a response team may decide to offer, with some discussion of each of these. The full list is available at: http://www.cert.org/csirts/services.html [1].

In the terminology of that document the services in Section 3 are as follows:

Basic Service	**Additional Functions**

Incident Handling (support or on-site)	Incident Handling on-site
Alerts and Warnings	Incident Response Co-ordination
	Announcements
	Security Related Information Dissemination
	Awareness Building

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/incident-response-functions

Links
[1] http://www.cert.org/csirts/services.html