Staffing models for incident responses

The basic staffing requirement of an incident response function is that there be some individual or individuals able to receive and respond to reports during the function's operating hours. The speed of response should be set as part of the function's agreed operating policy, however the working arrangements should allow for emergency situations where action to resolve a problem needs to take priority over all other normal work. Different organisations will find different ways to fulfil these requirements with the skills available to them; this section discusses a number of models that have been adopted by organisations on Janet and elsewhere in the world. More detailed descriptions of how these apply to particular case studies are in the next section.

Core Team

Some organisations are able to staff their incident response function with dedicated full time staff. This is commonly the case for teams with national or international coverage, but it can also be found in some universities. Such staff should quickly become experts in incident response, but it is important to ensure that they do not spend all their time on this stressful and often distressing work. Most staff appreciate spending time on more positive, pro-active work, such as helping to develop or install preventative systems. It is also important to ensure that such staff have the opportunity to maintain their technical knowledge and skills, as in a pure response environment the opportunities for this can be limited.

Rota

In some cases there may be organisational problems in dedicating staff full time to incident response as well as the potential problems of specialisation identified above. In these situations, and where the rate of incidents is not too high for one person to deal with, then a system based on a duty rota can work well. Here each member of the team spends part of their time dedicated to incident response and the rest working on some other job, for example systems administration in another department. A rota is arranged so that at all times at least one person is available to respond to incidents. This arrangement is particularly suited to organisations that already have a number of skilled staff working in various departments: these staff can be offered variety in their jobs through involvement in incident response, their departments should also see benefits through increased staff skills and awareness. Rota staff are likely to be familiar with the systems being used in their constituency as in the other part of their job they are likely to be running them. Expertise in incident handling is also more widely spread: if incident response takes one person’s worth of effort it will be easier to cope with holidays and resignations if this knowledge is shared between three or four bodies.

However a rota system needs good management agreements since the departments that ‘own’ the staff must release them for incident response duties according to the rota, whatever the current situation in the department. Competing priorities need to be resolved before they

occur, rather than in the middle of an incident. A rota system also requires good technical support systems as it is likely that some incidents will need to be passed from one member of the team to another as the rota progresses. This handover must not require the next person in the rota to rediscover all the information about the incident from the user who reported it! In particular any actions taken, planned or awaited must be recorded so this information is not lost in the handover.

Rotas are common in universities and colleges and at least one national team operates a very successful rota. Their procedure is even more of a challenge to the support systems since members of the rota are located at different sites with most communications and incident tracking being done electronically or by telephone.

Hierarchy

Many teams work with a more or less formal hierarchy of incident response roles, with incident responders taking calls and dealing with routine incidents, incident handlers taking responsibility for managing the smaller number of more complex or long-duration incidents, and technical experts available to advise for the few highly complex or novel incidents that need particular specialist skills. A particular individual may take on more than one role at different times: in a rota, staff who are not acting as incident responders at a particular time may be available as technical experts when needed; in a core team an individual may rotate through all three roles at different times.

A few large teams are able to have individuals permanently allocated to roles, with job descriptions to suit. Here there will usually be a training process to help staff to progress from incident responder to incident handler and technical expert should they choose to do so. Elsewhere the technical experts may be outside the organisation entirely, but with them and their organisations willing to use some of their time to benefit the wider network community.

Useful experts need not be restricted to those with computer and network skills: for example there can be great benefits to a team in having a ready source of legal or public relations advice. In all cases, experts should be made part of the team so they understand the aims and abilities of the operation. An informed expert who is not involved in the day to day running of the team can often make unexpected and valuable suggestions as to how the operation can be made more effective. As with the rota system, the use of external experts needs to be agreed in advance with details such as payment for equipment, expenses or time agreed.

Hybrid

In practice most teams use aspects of all three models to provide the best service from the available resources. It is vital that whatever arrangements are chosen there is clarity, both for staff and organisations, of what is expected of each individual. In particular where staff from outside the main incident response department or organisation are to be included, the arrangements for them must be the subject of detailed negotiation and agreement. Incident response must be done in a spirit of co-operation, however it is easy for the stresses of operational work to sour these relationships.

Out-of-Hours Cover

A few teams are required to provide incident response cover outside normal working hours,

either through a staffed office or having staff on call. The costs of setting up an out-of-hours operation should not be underestimated. Extra communications equipment is likely to be needed and some buildings may be completely unsuited as workplaces, for example if they are locked or unheated overnight. Additional staff will almost always be needed to cover the extra hours; contracts of employment for all staff involved are likely to need to be changed. The working arrangements for out-of-hours staff are subject to both national and European law. For a small number of callouts a rota team is likely to be the easiest to extend into out-of-hours calls as the on-call duties can be spread among a larger number of individuals.

Staff working out-of-hours also need to be delegated considerable authority to deal with problems. If a problem is reported overnight from a particular computer, network or site, then the out-of-hours staff need to be able to shut down or disconnect the apparent source of the problem. In some cases it will be necessary to disconnect the organisation from the Internet. Out-of-hours staff may also need to respond to or contact law enforcement agencies and possibly to give them access to the organisation. There is little point in incident responders being available out-of-hours if actions need individual authorisation from managers who can only be reached during office hours.

Co-operation

Few incident response teams are able to be wholly self-contained; in particular most will rely on their host organisation for administrative facilities such as finance and personnel. In planning a team it is also a good idea to consider what other parts of the host organisation may be able to contribute to incident response work, to avoid duplicated effort or conflicts where the functions of different groups overlap. In particular some of these external departments may have specialist skills or equipment that would not otherwise be available to the incident response team. Common examples are helpdesk, documentation, public relations and legal advice.

Staffing a helpdesk or call centre can require large numbers of staff, as well as telephone and request tracking systems, so if the organisation already has a helpdesk it may be more efficient to use this than to set up another solely for incident response. Callers may also find it less confusing if they have a single number to contact for all queries. However incident response calls are likely to require greater confidentiality than normal helpdesk business so staff need to be trained to deal with these; it may also be necessary to introduce additional protected fields into any request tracking system. A policy will also be needed for calls made directly to the incident response team: in some cases these may be justified in emergencies but staff should ensure that these calls are not lost from any tracking system.

Even the most basic incident response function is likely to involve public notices, if only to explain why a particular service is not available. As the incident response function grows it is likely to want to issue pro-active notices and information to improve the overall security of the organisation. In prominent organisations information security may well be a topic of interest to the press and badly handled publicity about a security incident can be damaging to the organisation's reputation. Equally, an organisation that has an effective incident response team may wish to publicise this fact. Preparing documentation and dealing with the media are specialist skills and not commonly found in incident response staff, however many educational organisations have departments with these specific roles. Working with documentation and public relations departments is likely to involve collaboration, with the different teams establishing an understanding of each other's roles and opportunities. Incident handling staff

with an interest in, and aptitude for, these areas should be encouraged to develop their skills, possibly through formal training, as technical staff who can also communicate effectively are very valuable in promoting security both within and outside the organisation. Information security incidents and investigations will often have legal implications for those involved and for the organisation. If not properly authorised and carried out, some of the activities of the incident response staff may even be crimes under current UK legislation to protect the individual, and may involve the organisation in civil or criminal liability. The incident response team should therefore ensure it is able to call on both informal and formal legal advice in developing its procedures and in dealing with individual incidents. This may be expensive if there are no in-house lawyers available, but should be supported by the organisation since, if things go wrong, it is much more likely that the organisation will be sued than individual members of staff. Although it cannot provide advice on specific circumstances, the JISC Legal Information Service (J-LIS) provides a considerable amount of legal information on its web site that is relevant to computer and network operations and investigations:

http://www.jisclegal.ac.uk [1]

In some cases it may be possible for incident response teams to work with others under informal agreements. Where special procedures need to be followed or priority access is needed then these may need to be established through more formal arrangements. Incident response work tends to involve emergency situations when processes need to work smoothly: how this is best achieved in practice will depend on the working culture within each organisation. In any case, some form of arrangement should be made and working relations established before they need to be called on in an emergency.

Links
[1] http://www.jisclegal.ac.uk