Published on *Jisc community* (https://community.jisc.ac.uk)

Incident response and policy

Organisational Policy

Incident response is a fundamental part of the organisation’s operation, playing a part in protecting both its services and reputation, so it must be included in the organisation’s policies and procedures.

The first aim of incident response is to limit the damage caused by an incident. Whether this involves shutting down a compromised computer or disconnecting a hostile network it will often involve a temporary reduction in the computer or network service available to some or all users. This will cause inconvenience to users, so it is essential that such action be authorised by the organisation’s management. In many cases it will be impractical, or too slow, to obtain this authorisation on a case by case basis, so common incident response activities, such as disconnecting a computer from the network or blocking a service at a router or firewall, need to be authorised in advance as part of the organisation’s security policy.

When the team starts to investigate an incident it must have the authority of the organisation to do so, or else it may be acting illegally. Both the Regulation of Investigatory Powers Act 2000 [1] and the Data Protection Act 1998 [2] state that certain actions may only be performed lawfully by staff who are properly authorised. The prescribed activities include things that will be required in most investigations: examining traffic on networks and looking at personal data in log files, e-mails or anywhere else. Employees who act without authority may be committing criminal acts and their employers may be sued for damages by those whose privacy is invaded.

Finally, teams that attempt to raise awareness and promote good security practice should find their work much easier if it has the formal backing of the organisation. For teams that wish to enforce good practice such backing will be essential.

Incident response teams can also be a useful resource in developing and improving security policies, as they have direct experience of security problems and whether existing policies are working. Developing and implementing policy should not be the responsibility of incident response staff alone, as management and users also have an essential contribution, but a policy is more likely to be practical and relevant to the real problems faced by the organisation if incident response staff are involved. In all cases, security policies must apply to everyone in the organisation. If anyone, be they senior management, system administrator, member of the response team or user, acts as if they are exempt from the organisation’s stated policy then the policy will be discredited and no one will see the need to follow it.

Incident Response Policy

As well as being part of the organisation's policy and procedures, the incident response function should also have its own internal documents to describe how it works. These documents should ensure that the team provides an efficient and effective service, whoever is involved. One of the most useful documents is an incident response plan that sets out the steps to be taken when an incident is reported. Since every incident is different it will not be possible to describe every last detail, but the various stages should be described. The plan should identify what steps can be taken within the routine authority of the team and in which cases (and how) individual approval needs to be obtained. Some incidents may need the assistance of others within and outside the organisation: typically public relations, legal departments and law enforcement agencies.

The processes for involving these should be described and, if possible, discussed with the bodies concerned to ensure that processes work when needed. The plan should identify what records are kept of communications and actions. These should allow an investigation to be handed over to another member of the team if needed and also record the actions taken if these are later questioned. A file of completed incidents can also be very useful as a resource for improving the team's effectiveness and identifying common problems in the constituency that may need to be addressed by awareness campaigns, changes in organisational policy or in the services offered.

Incident response staff are in a position of great trust within their organisation. They will routinely be expected to work with information that is sensitive both to the organisation and to individuals. The authority they need to do their job can also be abused to harm the organisation and the individuals within it. Incident response staff must always therefore work to the highest standards of professionalism and ethics, in particular not disclosing information they learn during the course of their work. Failure to maintain high standards will quickly result in the individual, the team and the organisation losing their reputations. Our suggested Charter for System and Network Administrators [3] describes a code of practice for administrators of individual systems and their managers.

Incident response staff should work to at least this standard and must have the full support of their management in doing so.

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

Links
[1] http://www.hmso.gov.uk/acts/acts2000/20000023.htm
[2] http://www.hmso.gov.uk/acts/acts1998/19980029.htm
[3] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html