CPNI
Centre for the Protection of National Infrastructure

10 OCTOBER 2007

FIRST RESPONDER'S GUIDE

POLICY AND PRINCIPLES

Version 1.3

Disclaimer

CPNI has taken every care in preparing this protective security advice, which is informed by intelligence on the threat. However, CPNI cannot accept any liability to any person or company for any financial loss or damage arising from the use of this advice or from any failure to give advice.

CONTENTS

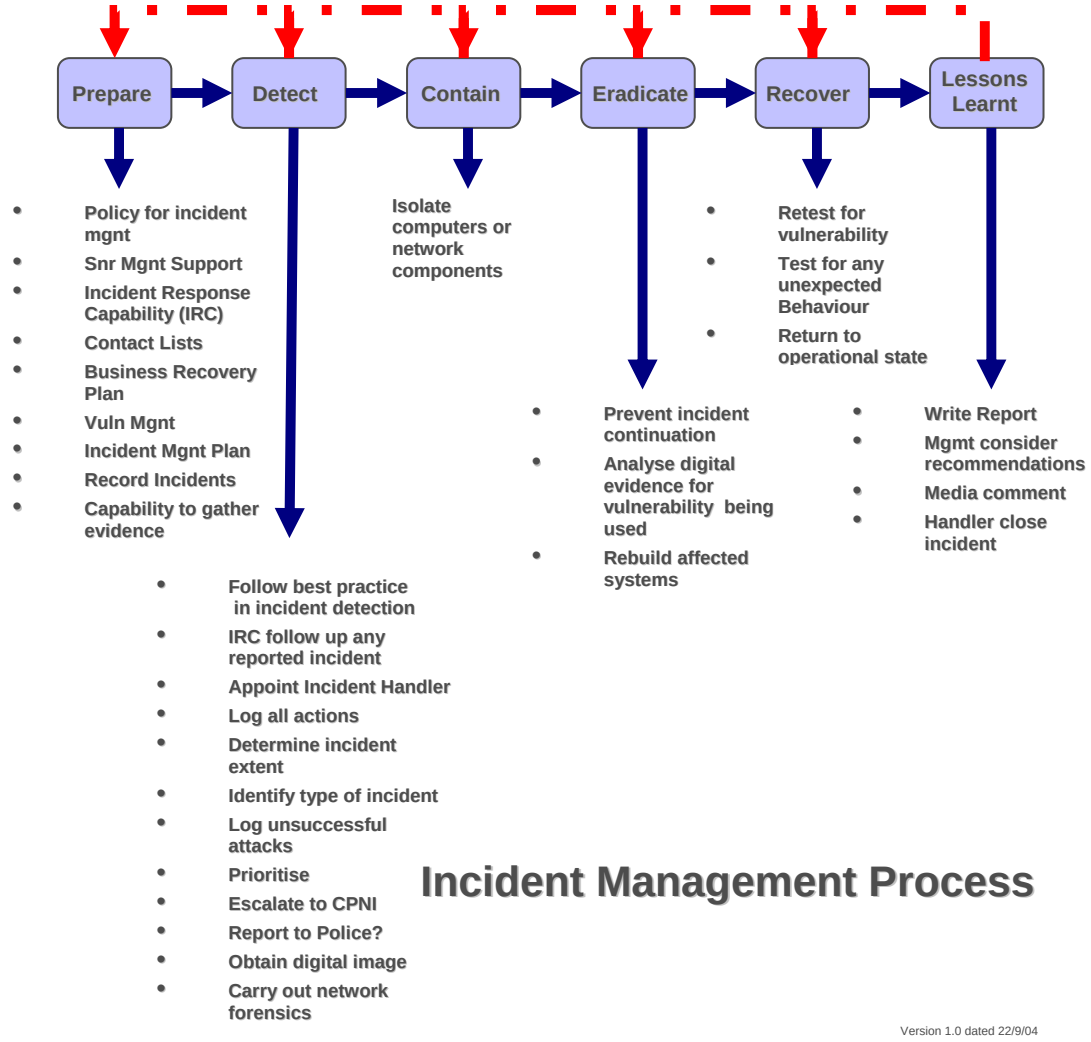
INTRODUCTION

This document sets out the policy that CPNI regards as best practice for response to electronic attack incidents and provides some general principles. Some notes are provided by way of justification but this document is not a detailed practitioners' guide. A companion document provides detailed advice on how to implement that policy.

The intended audience is IT security personnel and senior individuals who are likely to establish and oversee the work of an incident response team within their organisation. The emphasis is primarily on understanding and responding to business risks and what is required of an incident response team.

The guidance provided here is for use by UK Critical National Infrastructure organisations. The diagram below provides a summary of the methodology used in this document.

PRINCIPLES OF RESPONSE



- The responder's mantra: prepare, detect, contain, eradicate, recover and lessons learned
- Follow best current IT security practices: minimise vulnerabilities and their impact; apply patches after testing
- Minimise opportunity for abuse; use the principle of least privilege
- Be prepared for an incident: know who and how to manage the incident, and have a plan for system and data recovery
- Run incident management as a project, with members from different areas of the organisation
- If in doubt whether a system has been compromised, rebuild it.

PREPARATION

1. Organisations should have policies to assess the risk of electronic attack on their IT systems, including the business impact of attacks and should identify and implement countermeasures to reduce the risk of attack to an acceptable level

These policies may be assessed as part of an assurance report written by CPNI or as part of an ISO 27001 compliance audit.

2. Organisations should support a management structure that allows risks associated with electronic attack to be mitigated and a response to be made to any incidents reported

Best practice is to assign a senior executive at board level (or equivalent) or reporting directly to the board to oversee the assessment of security risks to the operation of the organisation. This executive will have knowledge of the business as a whole and is in a position to understand what comprises a manageable level of risk. Reporting to the executive will be security personnel who understand the security requirements of individual systems and who will co-ordinate the response to incidents affecting those systems. Incident handlers are likely to report to these individuals. Incident handlers have operational control over incidents. Further details are provided below.

3. Organisations should have an incident response capability or team with policies and operating procedures that are defined by higher management.

IT security incident response is a normal day-to-day activity within any organisation that forms part of the UK's critical national infrastructure. It is therefore important that these organisations establish policies and procedures for reporting and managing the response to these incidents. These policy documents will define the incident response team's management chain, responsibilities and methods of working. They will include information on such issues as media contact, legal advice and law enforcement, security and training.

An incident response team need only comprise designated individuals who are available to respond to incidents when needed, from the business management, business recovery, security, IT support, public relations and legal advice areas of the organisation. Different team members may be needed for different incident types. The additional cost of operating an incident response team need not be large (time, training and specialist tools); and in fact the benefit to the business of resolving an incident quickly may outweigh the additional demands on the individuals' time.

4. Organisations should have a contact list for members of the incident response team, for incident response teams of organisations that provide managed services to them, and a point of contact for the team.

The organisation needs to be able to contact the incident response team, and the team needs be able to contact its staff and those providing outsourced services in the event of an incident.

5. Organisations should have a plan for business recovery which should be regularly exercised.

The only sure way to recover after the compromise of an IT system is to rebuild the system and restore the data from a known good backup. Unless system restoration is practicable, incident response is likely to have high impact on business operation.

6. Organisations should actively monitor for new vulnerabilities and exploits that could affect their systems

Preparedness will help organisations minimise exposure to vulnerabilities and attacks that exploit those vulnerabilities. Monitoring vendor advisories, where they cover the technologies used by the organisation, and taking actions on this material relevant to the organisation (including mitigation or patching) are essential preparation steps.

7. The incident response team should have a way of assigning and managing priorities in responding to incident and a procedure for escalating the incident in order to engage business management

Priorities can be a useful way of resolving conflicts between resources where more than one incident is being handled at the same time. Higher priority tasks will be assigned resources in preference to lower priority tasks. Escalation procedures ensure that business management can make decisions on managing the impact of an incident on the business as a whole.

8. The incident response team should have a system to record all actions taken in respect of an incident and store that information for later retrieval

An incident recording system helps keep track of incidents and enable trends to be evaluated. Additional benefits are the ability to substantiate the cost benefit of incident response teams to an organisation, identify manpower and training requirements, and hardware and software needs.

9. All incident response teams should have the capability to gather evidence of the cause of an incident in such a way that it does not interfere with further investigations by internal or external agencies, e.g. law enforcement or the national security authorities.

Forensic investigation is work for a properly trained and equipped team. Incident response teams use tools that require specialist training including those for determining what processes are running on a computer, capturing network activity and for capturing and analysing digital images of computer disks. An inexperienced investigation team can destroy evidence or render it inadmissible in a court of law, thus significantly reducing the chances of a successful prosecution. Police guidance is available at:
http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

DETECTION

10. **All CNI organisations should at minimum follow best current practice in the detection of IT security incidents**

Some organisations will be required by dint of the sensitivity or criticality of information or systems to exceed the requirements of best current practice, but should at least use detection measures such as:

- Logging by firewalls, operating systems and applications
- File integrity checkers
- Intrusion detection systems
- Network traffic monitoring

Although these measures do have a financial and human resource cost, when these measures are deployed incidents will be identifiable.

11. The incident response team should investigate any incident or anomalous occurrence reported to it

12. The incident response manager should appoint an incident handler for the incident to manage all actions taken in respect of the incident

13. The incident handler should keep a detailed log of all actions taken in responding to the incident, including time stamps

The log can be used by investigators in evidence against an attacker.

14. The incident handler should determine the extent of the incident

15. The incident response team should identify the hosts affected by the incident (for example by unusual or malicious network or host activity) and the source of the incident

16. The incident handler should determine whether the incident report is a false alarm

This may involve checking logs and network traffic captures.

17. The incident handler should assign a priority to the incident in consultation with business management

18. The incident handler should attempt to determine the type of incident

Incident types that may occur include:

- Port scans & probes
- Denial of service
- Hacking attacks
- Virus/worms
- Data interception & monitoring
- Breaches of corporate security policy

19. The incident handler should determine whether the incident report relates to an unsuccessful attack or to a system compromise

Unsuccessful attacks should be logged for information and monitored, but no further action need be taken apart from reporting such incidents to, for example CSIRTUK, as part of routine course of business.

20. In the event of a successful targeted attack, the incident handler should report the incident to CSIRTUK.

CSIRTUK exists to provide assistance to constituents. It acts as a single point of contact and will, with the reporter's permission, inform other agencies that can assist in responding to the incident. Incidents can be reported to CSIRTUK via email at csirtuk@cpni.gsi.gov.uk.

Information on attacks can be used by CPNI to make assessments regarding attribution. CPNI request that no interaction take place with any Internet entities identified during the course of an incident investigation e.g. active probing of suspicious domains. Activity of this sort can alert the attackers to the fact that the compromise has been discovered, and result in them moving or changing infrastructure. This can impact on the ability of CPNI to form assessments regarding attribution, and to produce useful signature information.

21. The incident handler should ask the reporter whether the incident should be passed to the police for investigation

Successful hacking attacks contravene the Computer Misuse Act 1990 and denial of service may involve crimes such as extortion. Worms and viruses may also breach the Computer Misuse Act is they allow unauthorised access or make unauthorised modifications to data. The local police Computer Crimes Unit will advise on next steps if the organisation believes that a crime has been committed.

22. If the incident is a hacking attack or targeted malicious software, the incident response team should take a digital image of the computers' hard disks

The digital imaging should be performed in such a way as not to affect any files left by the attacker. This work does require specialist skills.

23. If the incident is a hacking attack or targeted malicious software, the incident response team should perform network forensics on the computers affected and capture the state of running processes

The network forensics should be performed in such a way as not to affect any files left by the attacker. This work does require specialist skills.

CONTAINMENT

24. The incident response team should isolate (for example physically disconnect from the network) any computer or networked device that is believed to be compromised by malicious software or a hacking attack

A compromised computer can cause further security problems if it remains connected to the network. Compromised devices can include routers, switches and firewalls as well as servers and desktop computers.

25. If a computer or networked device cannot be isolated individually, the incident response team should isolate the local area network to which it is connected

26. The incident response team should keep system users informed of their actions

It is extremely important to notify users of the likely impact of the incident.

ERADICATION

27. The incident handler should identify measures to prevent continuation of the incident

In the case of a denial of service, suitable measures would be identifying source of the denial of service, block traffic from the source and to use another address (network address or domain name). For a virus incident, disinfecting the virus and applying any missing patches would be suitable measures. For a hacking incident or a targeted malicious software incident, a system rebuild is required once the extent of the compromise is known. In the event that a known vulnerability has been exploited (whether by a hacking attack or by a worm) affected systems should be rebuilt.

Detailed advice on specific systems may be available from the CPNI if an assurance report has been undertaken on the system in question.

28. The incident response team should implement measures to prevent continuation of the incident

In the case where systems are rebuilt, data should be restored from the last known good back up. (A back up can be known to be good if it predates the incident and the data can be validated by another source, such as a paper copy, that is accepted as correct). Any missing patches should be installed on a rebuilt system, prior to being connected to a system that may still contain compromised hosts.

29. The incident response team should rebuild computers and networked devices that are believed to be source of the incident on a separate trusted network to the network that has been compromised

Separation of security domains can assist in preventing devices from becoming re-infected with malicious software or subject of another hacking attack.

30. The incident response team should analyse the digital evidence collected and determine the vulnerability exploited (if any) and the origin of the attack

This step should not be taken if the police are investigating, but analysis of evidence is useful in identifying further preventive measures and for assessing the threat to your systems. CSIRTUK may be able to provide assistance with this task.

RECOVERY

31. Once all eradication and prevention measures have been applied, the computers and networked devices should be retested for the presence of the original vulnerability

32. Once all eradication and prevention measures have been applied, the computers and networked devices should be tested for evidence that no unexpected or malicious behaviour is exhibited

33. Once all eradication and prevention measures have been applied and the devices have tested and found to behave normally, the devices may be reconnected to the network and/or returned to their original operational role.

LESSONS LEARNED

34. The incident handler should write a report on the incident for the organisational security officer including recommendations on any changes in security measures

In cases where the there is no effect on the system, viz where the incident did not lead to system compromise or security breach, no report may be necessary. However, the incident information should be kept for statistical purposes.

35. The business management need to consider the incident handler's recommendations and should address wider business practices that have been impacted by the incident

36. The public relations officer should consider if a statement to the media will be needed

Public statements can be beneficial if the effects of the incident are likely to be noticeable outside the organisation. The senior executive responsible for security is likely to authorise the release of information to the media.

37. The incident handler should close the incident when the incident is no longer active, all changes to the system associated with the incident have been removed and adequate preventive measures to prevent the incident happening again are in place

APPENDIX A: CHECKLIST OF POLICIES

Organisational Policies

Policy name	Reference in doc	Your reference
Organisational Security Policy	Clauses 1, 2	
Incident Response Policy	Clause3	
Media Handling Policy	Clause 3	
Business Recovery Plan	Clause 5	

Incident Response Policies

Policy name	Reference in doc	Your reference
Vulnerability & exploit monitoring policy	Clause 6	
Incident priorisation policy	Clause 7	
Computer forensics policy	Clauses 9, 22, 23	
User impact policy	Clause 26	