



Issued: 11 July 2008, updated August 2008

Incident Response Guidelines

Executive Summary

Upon discovery of a computer security incident, the officer in charge of an investigation needs to evaluate the situation and choose the most appropriate response. GovCertUK can assist government departments and organisations to effectively recover from and prevent the reoccurrence of network security failures. This guide can aid in categorising an incident, identifying its seriousness and the level of assistance GovCertUK can provide.

Computer Security Incidents

GovCertUK is responsible for providing support to Government departments in responding to computer security incidents. As described in section 9 of the Annex to the Data Handling Review "[Cross Government Actions: Mandatory Minimum Measures](#)", all departments must report network security incidents to GovCertUK. Cryptographic security incidents should be reported to CINRAS, while those relating to sensitive personal data should be reported to the Information Commissioner and the Cabinet Office.

There are many definitions of an incident. For the purposes of this document an incident can be defined as *any real or suspected event in relation to the security of data or computer systems*. This can include anything from a forgotten password to the successful access of confidential corporate data by a hacker. The assistance provided by GovCertUK depends upon the seriousness and the extent of the incident, combined with the ability of the reporting department to understand and respond to such an event.

Whatever the incident GovCertUK will endeavour to offer technical advice and assistance as required, supporting the prompt return to normal operations. Depending upon the nature of the incident this can involve log analysis, forensic imaging and analysis, malware analysis and reverse engineering, mitigation advice and general good practice guidance. GovCertUK offers a range of response support from telephone or email triage to on-site assistance as required.

Classifying an Incident

GovCertUK employ four categories of security incident. Key characteristics of each category include the severity of the impact on normal business and the possible compromise of sensitive or confidential material. This incident classification guide should enable an incident manager to assess the appropriate response, but it is not an exhaustive list. Please contact GovCertUK if unsure of the best category or most suitable treatment.

Those in receipt of the CESG Bookstore CD, or with access to CESG's GSi website, can refer to HMG Infosec Standard No. 1, detailing risk level and business impact level evaluation. This should assist in the analysis of the severity of the incident.

Incident Categories

Critical

These incidents will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security, affect mission-critical equipment or services, or damage public confidence in the government.

E.g. targeted attacks or loss of publicly available online service.

Significant

Less serious events are likely to impact a smaller group of users, disrupt non-essential services, breach network security policy, or affect the respect of government bodies and services.

E.g. website defacement or damaging unauthorised changes to a system.

Minor

Many types of incident can be capably handled by local IT support and security officers and do not require GovCertUK assistance, although GovCertUK should be notified of their occurrence. This aids the correlation of similar events, furthers the understanding of the IT security challenges facing government and may raise awareness of new attacks.

E.g. unsuccessful denial-of-service attack or the majority of network monitoring alerts.

Negligible Impact

It is not necessary to report on incidents of limited impact or those affecting only a few users. This sort of event would include receipt of isolated spam or anti-virus alerts, minor computer hardware failure, loss of network connectivity to a peripheral device such as a printer, or loss of access to an external non-essential service. In general these would be considered to be part of normal IT support operations.

E.g. isolated anti-virus alert or spam email.

Please refer to the categorisation look-up table and associated definitions below to assess the most appropriate response.

Incident Response Guidelines - Date: 11 July 2008

Incident Categorisation Matrix

Note that *these categorisations are general*; the extent of disruption, number of users affected, or the ability of local IT support to deal with the situation are all factors in assessing the appropriate category. If in doubt please contact GovCertUK for further information, clarification and assistance.

Network-Related Incidents

Incident Type	Desktop / Laptop / Mobile Devices	Server	Infrastructure – Multiple Systems Routers, firewalls, switches, hubs, wireless access points, etc
Targeted attack	Critical	Critical	Critical
Non-targeted attack	Significant	Critical	Critical
Loss of data affecting the security of the network, infrastructure or systems	Significant	Critical	Critical
Theft / loss of cryptography equipment or media	Report to CINRAS	Report to CINRAS	Report to CINRAS
Website defacement	N/A	Significant	N/A
DoS / DDoS – successful	Minor	Significant	Significant
DoS / DDoS – unsuccessful	Minor	Minor	Minor
AV alert / quarantine: widespread	Minor	Significant	Significant
AV alert / quarantine: single	Negligible impact	Negligible impact	Negligible impact
Network monitoring alert	Negligible impact	Minor	Minor
Spam	Negligible impact	Negligible impact	Negligible impact
Loss of public online service	N/A	Critical	N/A
Unauthorised access	Minor	Significant	Critical
Damaging unauthorised changes to system hardware	Negligible impact	Significant	Significant

Other Incidents

Incident Type	Large Central Government Department	Smaller Department or Local Government
Phishing (fraud involving misuse of branding)	Significant	Minor
Employee abuse of privileges or security policy (e.g. emailing login credentials)	Minor	Minor
Copyright infringements or piracy	Individual departments' responsibility	Individual departments' responsibility

Definitions

Targeted Attacks

A targeted attack can be considered as one where individuals or the victim organisation are intentionally chosen. This can include email based attacks with malicious attachments, website defacements, Denial of Service attacks, or unauthorised access to data and services. Full descriptions of these are available below.

GovCertUK consider all forms of targeted attack (whether successful or blocked) as of critical importance. Government bodies should always report targeted attacks to enable us to better understand and monitor attacker activity and to detect trends across government bodies.

Non-targeted (“drive-by” or spam-carried) Attacks

A non-targeted attack is one where the attacker has limited control over who the victims are and to the attacker this is immaterial. These often take the form of a “drive-by” attack, where legitimate web sites have been compromised and now host malicious code. Malicious code can also be delivered by spam email or by users following links in such email. This code can exploit vulnerabilities in the user’s system often causing the download and execution of “malware” (malicious software, including most adware, spyware and viruses).

Where such an attack has been successful (i.e. a computer has been compromised or malware has been executed) GovCertUK should be informed. It is not necessary to report cases where execution of such software has been prevented or blocked, for example through security software or computer policy settings.

Loss of Data Affecting the Security of the Network, Infrastructure or Systems

This refers to the loss of (a copy of) data that compromises the security and integrity of the network and may be a result of theft or loss of data-containing equipment or media. Such data includes lists of users, user names, passwords, digital certificates, authentication devices, network diagrams and documentation.

Website Defacements

Vulnerabilities in either website-hosting systems (web server) or the web site itself can allow an attacker to change content and pages. Such an attack may involve the insertion of links to malicious sites, adding malicious scripts or changing the content to carry the attacker’s message (which may be political, defamatory, for kudos or to damage the reputation and brand of the victim organisation).

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

The intent of a DoS or a DDoS is to disrupt a service or system. This may be achieved by exploiting a vulnerability in the victim’s infrastructure, causing it to crash or become dysfunctional. More commonly an attacker would swamp the infrastructure with large volumes of network traffic in an attempt to consume all available resources. The result is that the system is not able to service legitimate traffic or requests.

A DDoS attack differs from a DoS in that the traffic originates from multiple endpoints in a coordinated manner as opposed to a single attacking machine. A DDoS has the potential to consume greater resources through the use of many computers operating together, for example Botnets (a collection of compromised computers under the control of an attacker) or large numbers of Cyber activists working together.

Isolated and unsuccessful denial-of-service attempts that do not cause disruption and are no longer on-going need not be reported.

Incident Response Guidelines - Date: 11 July 2008

Anti-Virus Alert / Quarantine: Widespread

This relates to AV alerts across the enterprise where multiple systems have been infected. The severity depends on the specific alert, the infrastructure affected and the success in containing any infections. Contained infections with known causes need not be reported.

GovCertUK recommends using the resources available from the AV software vendor to understand specific alerts and to judge the impact and severity.

Anti-Virus Alert / Quarantine: Single

As above however a single client, server or device is affected.

Network Monitoring Alert

This includes alerts from Intrusion detection systems (IDS), Intrusion prevention systems (IPS), Web filtering products and email scanning services.

The severity depends on the specific alert and the frequency. Some of these alerts may relate to a number of high severity incidents such as Targeted Attacks. However, they may also detect the usual background network activity all Internet-facing systems and services will experience, such as probes, port scans and spam.

GovCertUK will consider high severity alerts or alerts which correlate with a successful attack as an incident. Using vendor resources or information relating to the specific alert should be considered before reporting an incident.

Spam

Spam is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk email messages.

GovCertUK does not need to be informed of the receipt of spam mail. However, if it is discovered that a Government system is sending spam mail this may indicate a successful compromise and should be reported.

Loss of Public Online Service

This may be the result of DoS or DDoS or a similar Targeted Attack, although it also includes the loss of online services through exploitation of vulnerabilities in the web application or server platform. This could also cause the loss or disclosure of data hosted within the online service.

Unauthorised Access

Evidence of unauthorised users from outside the department or organisation gaining access to data or services signifies a compromise of system integrity. This may be the result of a targeted attack and can include access to user accounts, user account administration and data exfiltration.

GovCertUK should be informed of incidents where unauthorised access is gained from outside the organisation; where such access is gained within the organisation, departments should at the first instance follow their usual internal security procedures.

Damaging Unauthorised Changes to System Hardware

This is where an individual not associated with the organisation is able to gain physical access to system hardware and make unauthorised changes. GovCertUK can offer advice on how to recover the affected network or system from such changes; it is advisable to contact the Centre for the Protection of National Infrastructure (CPNI) for advice on how to prevent future unauthorised physical access to the system. Theft should be reported to the Police or local law enforcement body.

Other Incidents

Phishing

This can be considered as an attempt to criminally and fraudulently acquire sensitive information such as usernames and passwords or other personal information to allow an attacker to masquerade as a legitimate user and obtain access to services and accounts. Where a particular user has been targeted it is usually called "spear-phishing".

In this context an incident is defined as a service or account owned by a Governmental department being used as the lure of a phishing fraud, rather than users receiving phishing emails attempting to solicit details for external organisations e.g. Online banking etc.

Employee Abuse of IT Privileges or Security Policy

Despite educating users in IT security, many attempt to circumvent security mechanisms. This includes changing user settings or computer configuration, altering programs so they might pass through email filtering software, or sharing what should be private login credentials to another party. The majority of these cases should be within the remit of an individual department's security policy and enforcement procedures. If, however, it is suspected that the availability, integrity and confidentiality of an essential system or public service has been seriously impacted by such actions then GovCertUK can assist in recovering its security.

Copyright Infringements or Piracy

The misuse or unauthorised replication of published or patented material is a legal matter between the copyright or patent holder and those responsible for its infringement. The affected group or department should address the matter themselves, following advice from the UK Intellectual Property Office.

GovCertUK is responsible for Computer Security Incident Response within UK Government, and provides an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents.

The CESG GovCertUK Incident Response team provides 24 hours a day, 7 days a week operation and can be contacted by the following methods:

Telephone:	01242 709311
Fax:	01242 709113
General Enquiries:	enquiries@govcertuk.gov.uk
Incidents & Alerts:	incidents@govcertuk.gov.uk
Restricted communications (GSI only):	govcertuk@cesg.gsi.gov.uk
Website:	www.govcertuk.gov.uk