

INFORMATION SECURITY: INCIDENT HANDLING CHECKLIST

The following is a series of practical steps you can take when faced with a live information security incident. Many of the actions are common sense (if they seem simplistic, they are!) and will also help your organisation in matters unrelated to information security. The actions are divided into '[Preparatory Steps](#)' and '[Response Steps](#)'.

Preparatory steps

- Collect the contact details of all people likely to be required in the event of a major incident. Make sure you keep multiple copies of this information off site and that major players keep it to hand.
- It is worth setting up a specific telephone number for people to use during major incidents. This might even be a mobile since the incident may prevent you from accessing your normal telephones. Some companies set up a Freephone number (0800 or 0500) so staff can get in contact or listen to a recorded message updating them on an incident.
- Set up a web-based e-mail account(s) for use in emergencies. These accounts are both freely available (such as Hotmail) and are provided by commercial Internet Service Providers (such as BT Internet). Use these facilities to inform those who need to know what's happening should your normal e-mail capability become unavailable.
- If your organisation is highly mobile, use facilities such as SMS (text messaging) to keep staff up to date. Many services allow you to send texts to multiple numbers, often via a web page.
- Keep a list (on and off site) of those external people/organisations you should contact in the event of your business becoming inoperable, or if normal channels of communication are broken. These could include:
 - police (local and national)
 - insurance companies
 - lawyers
 - trade associations
 - Inland Revenue
 - major clients
 - local government.

Response steps

- If the incident affects your ability to deliver goods or services, tell your customers as soon as possible. They will probably prefer to be informed up front rather than have to face a late or cancelled delivery.
- You should try to contain the incident and record its timing, duration and location. You should also:
 - find out whether the incident is ongoing; and
 - Determine whether you need to isolate systems that have been affected (this is important in the case of computer virus infection).
- If the incident could result in a police investigation (i.e. if a crime is suspected), you should not interfere with the scene. Take photographs and record evidence of system connectivity etc. You should also:
 - create a 'forensic' backup of relevant data or systems, e.g. 'imaging' of computer systems to provide evidence; and

- identify what records/logs/evidence of the incident exist, including witnesses, CCTV and manual systems.
- The next major response phase is to assess the damage caused. Perform the following steps:
 - determine the extent of damage or penetration;
 - interview witnesses or relevant parties (including service providers etc.);
 - gather supporting evidence e.g. penetration test reports, network reviews, gap and risk assessments; and
 - gather staff evidence, e.g. HR records.
- You should then start performing recovery activities. In the event of a technical incident (such as external ‘hacking’), perform appropriate technical upgrades, introduce patches, carry out a configuration review, harden your network protection, review your intrusion detection devices and appraise your policy.
- Take the opportunity to revise policy and staff training, determine HR and contractual issues (to include external suppliers) and review outsourcing agreements (as appropriate).
- You should also start to manage PR and publicity issues, e.g. with staff, customers and shareholders. You should involve appropriate external parties as necessary, e.g. the police, relevant regulatory bodies and insurers.

NB: It is important that you communicate with your staff. People react badly when they are not kept informed. Even negative feedback is welcomed, provided people know the situation and feel they are being considered. Exclusion is almost always negative.

Please refer to the guidance on [Incident Management](#) in our business advice pages (see below) for further information.

Further help and advice

General

BERR Information Security Health Check Tool
<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page
www.berr.gov.uk/sectors/infosec

BERR Information Security Business Advice Pages
<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)
<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>

Published by the Department for Business, Enterprise and Regulatory Reform
www.berr.gov.uk
© Crown Copyright. URN 09/651.