Information security incident handling procedure

Issue sheet

Document reference	NHSBSAIS003a
Document location	S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review of IS Policy\Current and Final
Title	NHS Business Services – Information security incident handling procedure
Author	Gordon Wanless
Issued to	NHSBSA Information Security Staff
Reason issued	For action
Last reviewed	16 April 2015

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Initial release	27.1.2011	-	**IGSG**	-
a	20.03.2014	C Dunn & C Gooday	ISF	Insertions made to introduction and Appendix to reflect PCI DSS compliance
b	16.4.2015	C Gooday	HOIG	Reflect current practice
c	21.10.2016	C Gooday	ISF	Update HSCIC name and also SUI to SIRI

Contents

Appendix

1. Introduction and scope

This procedure provides guidance on the handling of security incidents, breaches or suspected incidents and breaches.

The scope of this document is limited to those security incidents that affect the NHSBSA only.

The reporting of security incidents is covered in the procedure titled 'NHS Business Services Authority Information security incident reporting procedure'. This procedure is solely concerned with the handling of reported security incidents.

A high risk incident is defined as a Serious Untoward Incident (SUI) Level 2 or higher in the HSCIC IG & Cyber Security SIRI Checklist, where a cardholder breach occurs or an unauthorised wi-fi network is detected.

2. Incident containment

The underlying aim of the Containment stage of the handling process is to limit the actual and potential impact of the breach.

There are three key elements of containment:

- limiting the impact of the breach
- preserving the evidence of the breach
- controlling awareness of the breach.

The incident handling team will be engaged should a high risk incident occur. This will be coordinated by the Head of Internal Governance (HOIG) and the Business Continuity Manager. They will engage key staff that may include:

- System/Business owners for the area impacted.
- Information Security Manager
- Technical Assurance
- IT Providers and Security Personnel
- Service Stream Managers

- Communications Team
- Leadership Team

The incident handling team will assess the situation and consider the need to deploy the IT disaster recovery or business continuity procedures

2.1 Limiting the impact

Action taken to limit the impact of a breach will rely heavily on a person's understanding of the risks and issues involved. For example a System Administrator will understand the need to quarantine a virus infected client. Similarly, a member of the security team might take the decision to evacuate areas of the site following discovery of a suspect package.

2.2 Preserving the evidence

When taking action to limit the impact of an incident, care should be taken not to destroy or disturb any evidence which might later help in the identification of its cause. Controls should be put in place to prevent other staff from likewise interfering with evidence.

2.2.1 Evidence identification log

The evidence log provides a reference point for all incidents in which evidence has been recorded. All evidence identified following an incident should therefore be recorded. This will allow an auditable record to be maintained of all evidence associated with an incident. All evidence collected under the respective security incident must be referenced under the relevant 'Evidence no'.

The format of 'Evidence no' must be in a sequence concatenated to the security incident number, for example: if 3 items of evidence have been collected for a security incident with number 123, the Evidence Numbers on the Evidence Identification Log must read 123A, 123B and 123C.

2.3 Controlling awareness

There are a number of reasons why controlling the "sphere of knowledge" about an incident may be vitally important. A failure to do so may seriously impact the speed of an incident's resolution and the viability of any subsequent investigation. The following factors should be considered:

- **Avoiding panic -** Certain types of incident such as bomb threats and fire evacuations have the potential to cause panic where information about the situation is not properly controlled. Rather than giving guidance that is hasty and ill-considered, the steps of *Detection* and *Confirmation* (see above) should occur wherever there is sufficient time. A delay in releasing information may also be desirable in such circumstances to allow other measures to be put in place e.g. Evacuation-Coordination Teams or Fire Warden organisation.

By limiting knowledge to such a group the risk of the relevant facts and issues being obscured by misinformation and unqualified advice are greatly reduced.

- **Maintaining confidentiality** - During any incident there may be sensitivity issues to be considered (from both a commercial and legal/regulatory perspective.) In dealing with an incident staff should always be wary of taking action which might: compromise protectively marked material; result in unnecessary negative publicity or otherwise cause commercial embarrassment. Although these considerations of confidentiality are secondary to the concerns of system integrity and the safety of staff, they are nonetheless important factors.

3. Incident resolution

Once the incident has been identified and contained, efforts can then be focused on finding an appropriate solution. The fundamental features of any solution should be investigation, action (and follow-up/record-keeping.) The order in which they are implemented depends upon the nature of the incident.

The HoIG, assisted by the NHSBSA Information Security Manager (ISM) and/or the NHSBSA Information Governance Manager will initiate the appropriate investigation.

On receipt of the incident form the IG team will log the incident onto the information security incidents register.

After entering the incident details into the Central Register /Evidence Identification Log the incident reporting form will be forwarded to the relevant business area to initiate the appropriate investigation.

3.1 Investigation

Wherever possible there should be a thorough investigation into the cause and extent of a breach *before* any corrective action is taken. Attempting to fix a problem that isn’t properly understood creates a risk of exacerbating it. Once the situation has been suitably analysed, a solution should be devised and implemented through the coordination of technical, security and management resources.

The ‘Final Incident Report – Template’ on the Hub provides a useful framework to document the findings.’

In certain circumstances the need for action will be significantly more urgent, meaning that the amount of investigation time available is limited. In such circumstances qualified individuals may take *immediate* action (ideally with management authority) to solve the problem. An example of this would be where a cyber security breach has been identified and contained, and an immediate solution is available to restore the system (e.g. vulnerability patch.) System Administrators might feel that in these circumstances the overriding requirement of “system availability” warrants implementation of the solution before a full investigation into the breach can take place.

3.2 Action

What action is to be taken in solving any particular security incident will depend upon:

- the results of the investigation (see above)
- guidance given in the specific incident procedures
- the judgement of qualified individuals on the scene.

Where the solution to be implemented may potentially cause disruption to system processes or loss of data, all efforts should be made to provide an adequate “back-out” plan.

Some incidents may be serious enough to be a disciplinary offence. Where three incidents are recorded against the same individual then this amounts to a disciplinary offence. Such offences invoke the NHSBSA disciplinary procedures. For a high risk incident, the HOIG will discuss the incident findings with the SIRO. A decision will then be made as to the action required.

Such action needs to adhere to the NHS Digital SIRI procedures mandated for NHS organisations.

3.3 Follow-up

Once a solution has been implemented and the incident closed, it is vital that time is taken to learn lessons. There should be a debriefing involving all relevant parties to answer the following questions:

Review questions

- Is their a consensus as to the cause of the incident?

- Were there any specific weaknesses that allowed the incident to occur / worsen?

- How quickly was the problem detected / confirmed?

- Were there any communication problems encountered in reporting the incident? How might these be solved for future incidents?

- Was the incident limited as quickly and effectively as possible? If not what else might have been done?

- Was any evidence about the incident lost due to procedure failure? How might useful information about the incident have been better stored (or backed-up)?

- Was awareness of the incident properly contained or controlled? What effect did any “leakage” have on the handling of the incident?

- Were any other important issues raised during the incident that need to be included within the procedure?

All reported incidents will be re-evaluated at the next Information Security Forum to ensure the type of incident is no longer being reported or the volume of those incidents has dramatically reduced. If there is no change in the volume of each type of incident the IGSG will be alerted and appropriate action taken. This could be, for example, further training courses for staff or an improvement to existing security and / or confidentiality arrangements.

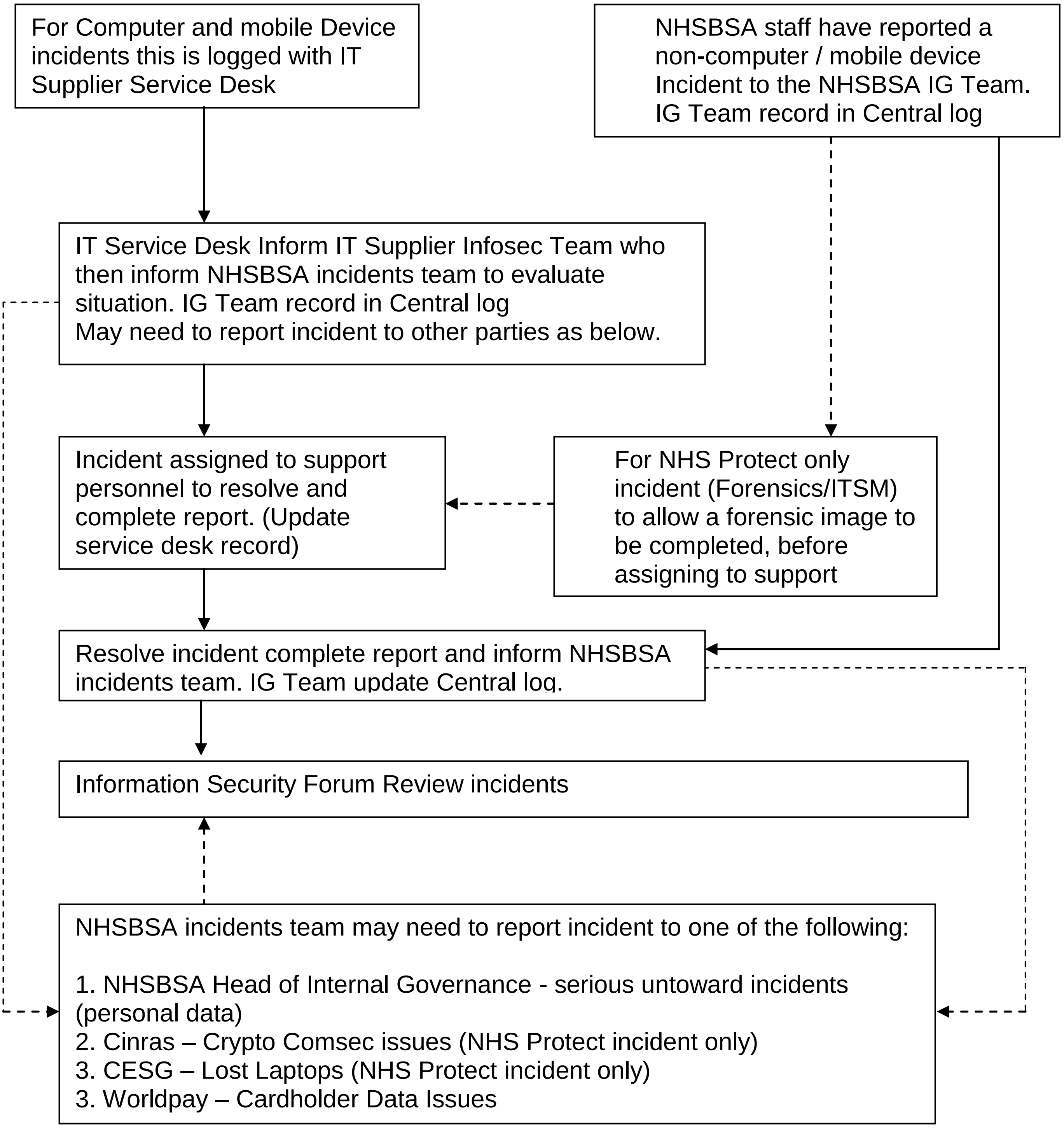
Incidents may be used in training sessions about security and confidentiality as examples of 'real life events' relevant to the NHSBSA which can then be more easily related to by staff. This gives attendees examples of what can occur, how to respond to such events and importantly how to avoid them in the first instance.

3.4 Record keeping

Once an incident has been investigated and reviewed, the record the central information security incidents register will be updated. Any related IT service desk calls will be closed off.

Appendix A

Flowchart



For Computer and mobile Device incidents this is logged with IT Supplier Service Desk

NHSBSA staff have reported a non-computer / mobile device Incident to the NHSBSA IG Team. IG Team record in Central log

IT Service Desk Inform IT Supplier Infosec Team who then inform NHSBSA incidents team to evaluate situation. IG Team record in Central log
May need to report incident to other parties as below.

Incident assigned to support personnel to resolve and complete report. (Update service desk record)

For NHS Protect only incident (Forensics/ITSM) to allow a forensic image to be completed, before assigning to support

Resolve incident complete report and inform NHSBSA incidents team. IG Team update Central log.

Information Security Forum Review incidents

NHSBSA incidents team may need to report incident to one of the following:

1. NHSBSA Head of Internal Governance - serious untoward incidents (personal data)
2. Cinras – Crypto Comsec issues (NHS Protect incident only)
3. CESG – Lost Laptops (NHS Protect incident only)
3. Worldpay – Cardholder Data Issues