October 2015
Issue No: 1.2

Good Practice Guide

Security Incident Management

Customers can continue to use this guidance. The content remains current, although may contain references to legacy SPF policy and classifications.

CPNI
Centre for the Protection
of National Infrastructure

CESG
NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Good Practice Guide No. 24

Security Incident Management

Issue No: 1.2
October 2015

Document History

Version	Date	Comment
1.0	August 2010	First issue
1.1	November 2012	Updates to reflect changes to SPF mandatory requirements numbering, and to references to other IA policy documents. Updates to reflect the newly available “Cyber Incident Response Service”
1.2	October 2015	First public release.

Executive Summary

In today's world security incidents are inevitable and when they occur organisations need to act swiftly to identify, assess and manage the response. A pre-planned, coordinated and well-rehearsed approach, supported by senior management, will minimise the business impacts of such events.

An organisation's response to Security Incident Management needs to be proportionate not only to its risk appetite but also to the costs of maintaining the Incident Management capability. Small organisations in particular will have to look carefully at the implementation options to ensure the appropriate capability is available in an affordable manner.

In some cases organisations will have to follow prescribed legal or regulatory procedures to manage and/or report incidents or will have chosen to adopt similar, recognised national or international standards.

Security Incident Management is a process aimed at minimising the immediate and long-term business impact of incidents. Benefits of investment in Incident Management should include:

- improved resilience and assurance of business continuity
- Increased reputation and customer / stakeholder confidence
- Direct financial benefits including reduced financial risk profile

All organisations face a range of security threats and vulnerabilities. These should be assessed so that they can be identified and managed. An organisation's response to the risks will be dependant on its risk appetite. However, no matter how conservative that appetite is, a residual element of risk will remain.

Incidents may have a wide range of causes and their impact will vary dependant on their nature, scope and severity. An inadequate response will almost certainly compromise the aims of Security Incident Management. A holistic approach to managing security incidents is also more likely to optimise business benefits and provide broader context within which to apply lessons learned and so reduce future risk exposure.

A limited number of managers and staff will be responsible for operating the security incident management process but everyone carries a responsibility to reduce the chance of incidents occurring and needs to be aware of how to react as a first responder.

Purpose & Intended Readership

This Good Practice Guide (GPG) aims to provide guidance on factors to consider in relation to the management of security incidents within organisations and to help develop and implement the policies and procedures needed to manage security incidents effectively. It is primarily targeted at security managers who are accountable or responsible for implementing security incident management. The emphasis is on understanding and responding to business risks and what is required of a security incident response team.

It has been written to be relevant to government and commercial sectors and treats the management of security incidents in a holistic manner, and identifies the main principles to be applied in any situation. This generic guidance is placed into context for HMG organisations in Annex A and for CNI organisations in Annex B, and the annexes provide more detailed guidance on the specific requirements, activities, documentation and points of contact for each sector.

The guide does not aim to duplicate existing published material; references and suggestions for further reading are used to direct readers to such guidance.

The guide does not reduce or absolve in any way an organisation’s responsibility to make decisions on how to implement good practice and establish a Security Incident Management System proportional to their business environment and risk appetite. Some organisations may already have localised detailed procedures in place and this guide provides a possible reference for their review.

Changes from the Previous Issue

Updates to reflect changes to SPF mandatory requirements numbering, and to references to other IA policy documents.
Inclusion of reference to the Cyber Incident Response Service.

Contents:

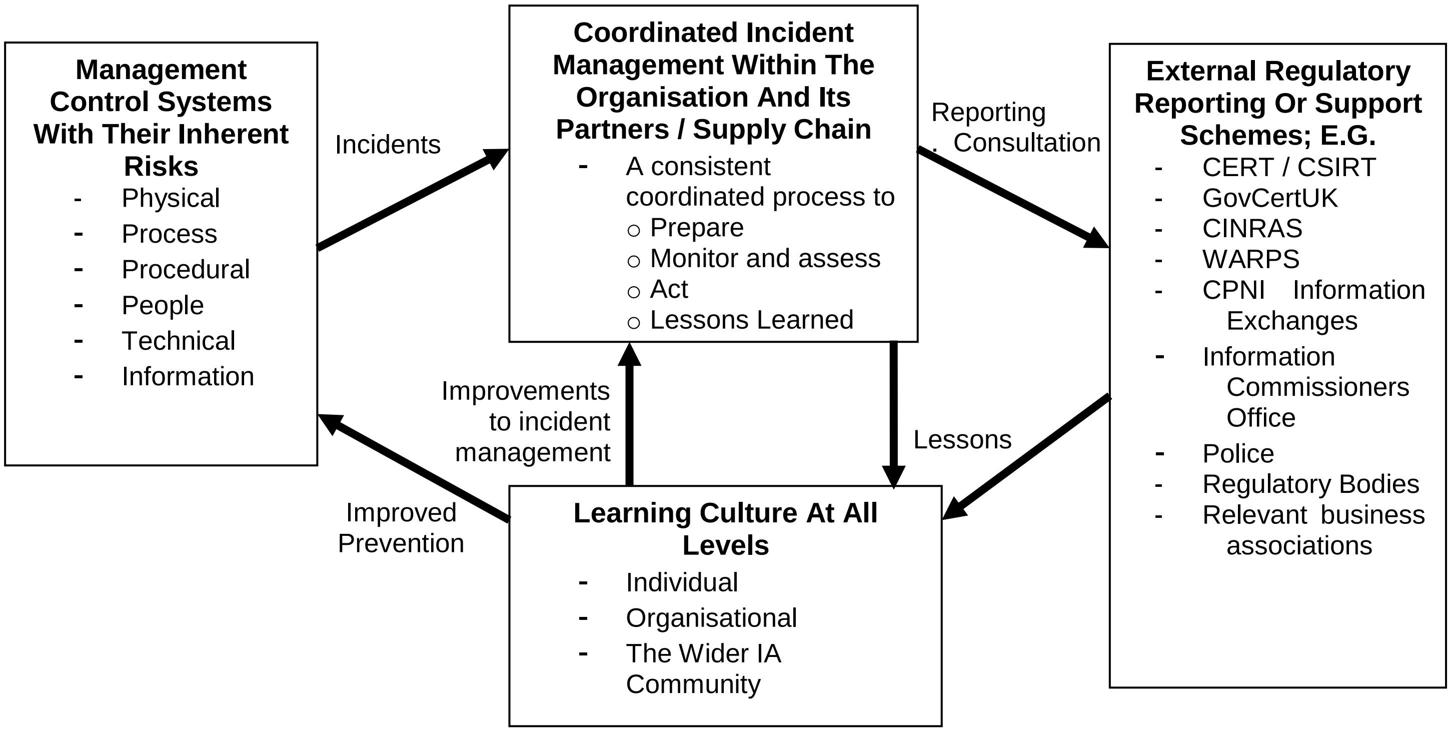
Chapter 1 - Introduction and Overview

Key Principles

- Security Incident Management is a critical activity for all organisations and all members of an organisation have a role to play
- An holistic approach to Security Incident Management is more likely to deliver optimum business benefits
- There is no single solution to fit all organisations but there is a consistent set of factors to be considered by any organisation when determining its approach to the management of security incidents

A Holistic Approach

1. Organisations are increasingly reliant on critical business assets whether they are personnel, information, technical or physical. Inter-dependencies between these groupings can lead to weaknesses in security controls in one area inevitably affecting other areas. Holistic coordination of controls and of response to security incidents is fundamental to effective incident management.



Management Control Systems With Their Inherent Risks
- Physical
- Process
- Procedural
- People
- Technical
- Information

Coordinated Incident Management Within The Organisation And Its Partners / Supply Chain
- A consistent coordinated process to
  - ○ Prepare
  - ○ Monitor and assess
  - ○ Act
  - ○ Lessons Learned

External Regulatory Reporting Or Support Schemes; E.G.
- CERT / CSIRT
- GovCertUK
- CINRAS
- WARPS
- CPNI Information Exchanges
- Information Commissioners Office
- Police
- Regulatory Bodies
- Relevant business associations

Learning Culture At All Levels
- Individual
- Organisational
- The Wider IA Community

Definition

2. Security Incident Management is a process aimed at minimising the immediate and long-term business impact of incidents. Within this overall aim specific objectives can be defined as to:

a. Establish the authority and responsibilities of those involved in the process.

b. Comply with legal and regulatory requirements.

c. Define and allocate responsibilities for incident management in specific policies and procedures, with copies held off-site.

d. Identify the sources and types of potential security incidents and manage the likelihood of them occurring.

e. Be prepared for handling incidents before they occur by implementing detailed incident management procedures including the provision of appropriate training.

f. Deploy effective detection techniques to identify incidents early.

g. Deploy effective incident reporting procedures to meet organisational and external reporting requirements.

h. Respond effectively and efficiently to restore business operations whilst preserving sufficient forensic evidence to sustain any legal or disciplinary processes.

i. Ensure effective security is maintained during the life of the incident.

j. Record all actions and decisions taken.

k. Communicate effectively with all stakeholders.

l. Ensure lessons learned are captured and acted upon including the analysis of any trends and patterns that may emerge.

Scope

3. Security incidents will occur in any organisation. Whilst many are likely to be trivial all must be managed effectively; trivial incidents can, on further inspection, be indicative of more severe underlying problems. In extreme cases failure to manage incidents effectively can lead to major disruption of business operations, litigation, extensive cost implications or even corporate failure.

External Accountabilities and Standards

4. Senior managers are accountable to stakeholders and have to report formally on the protection of business assets and maintain expected levels of business operation. Accounting Officers in HMG Departments are accountable to the Cabinet Office and Ministers; Business leaders in CNI organisations are accountable to Regulatory Bodies and Shareholders. Each have specific reporting requirements to maintain oversight of that accountability framework.

5. In addition to regulatory accountabilities as outlined above organisations are expected to address accountabilities to customers for levels of service and appropriate protection of their information. Organisations need to have a clear view of all stakeholder groups and a communication strategy that enables effective communication as and when required

6. Recognised standards are available to provide levels of assurance over the quality of the incident management process. The International Standards Organisation (ISO) and the European Network and Information Security Agency (ENISA) provide internationally recognised standards and advice. (Note: specific references are provided at the end of this guide)

Chapter 2 - Why we need Incident Management

Key Principles

- Organisations need a comprehensive and repeatable risk assessment process that identifies critical assets and related threats and vulnerabilities and enables an assessment of the potential business impact should any incidents occur
- Organisations need an Incident Management capability to minimise the business impact of any incidents that do occur
- A clear business case will focus on specific business outcomes that justify the investment in Security Incident Management capability

Introduction

7. This chapter outlines the business drivers for maintaining an effective Security Incident Management capability. The benefits of Security Incident Management and the balance with the associated costs need to be considered carefully in the context of individual organisations. Some general pointers on the risks of not having such a capability are listed.

Business Case

8. Effective Security Incident Management is an essential element of a wider business continuity requirement. The business case is rooted in the potential business impact that incidents might have combined with the risk appetite that an organisation is comfortable with. Some information can be gained from the cost impact of managing incidents that have occurred; this should include assessment of actual costs incurred and potential costs avoided. However, a more complete analysis is needed that links all assets used to specific services an organisation delivers or relies on. This should be correlated with the threats and vulnerabilities to identify and assess the potential business risks. Use of a recognised method will produce reliable and repeatable results. Independent published data can provide a useful source of estimated costs/ savings.

9. Such a process will enable organisations to specify business benefits sought from Security Incident Management. Benefits should be measurable in financial terms to justify initial and ongoing investment in Incident Management and should include such areas as:

   a. Proven ability to recover from incidents quickly and completely, leading to improved resilience and assurance of business continuity;

   b. Increased reputation and customer / stakeholder confidence;

   c. Direct financial benefits including reduced financial risk profile.

Business Benefits of Maintaining Effective Security Incident Management Capability

10. An organisation that has an Incident Management capability will be able to manage better its business risks such as:

a. Breaches of legal / regulatory requirements; eg loss of accreditation status of an HMG IT system.

b. Loss of Confidentiality, Integrity or Availability of systems or data;

c. Delayed restoration of business services with associated costs;

d. Loss of reputation / credibility with customers, possibly leading to lost business;

e. Direct economic losses –e.g. from failure to detect fraud, failed legal action, penalties due to breaches of legal / regulatory requirements, inability to make insurance claims, liability to others for compensation of consequential losses;

f. Destruction of forensic evidence (perhaps breaching legal requirements);

g. Inefficiencies due to prolonged and/or poorly coordinated incident management activity;

h. Recurrent incidents through lack of identifying root causes and applying lessons learned;

i. Reduced ability to obtain requisite insurance cover.

11. If any of these risks materialise there are potential cost penalties which may vary from a few tens of pounds for dealing with a single malware incident to millions where an Ecommerce organisation suffers a determined Denial of Service attack on their network connectivity or websites. If organisations are to maintain a robust business case to sustain incident management capability it is important that they understand the true cost of an incident and can estimate the likely cost savings that effective incident response has provided. Various organisations regularly produce a variety of statistical information that can support the drafting of business cases.

Chapter 3 - What is Needed – Common Principles

Key Principles

- There are five significant principles that organisations should observe to develop and operate an effective Security Incident Management capability. These are:
    - Compliance with Legal or Regulatory Requirements
    - Business Ownership
    - Planning
    - Information Management
    - Continuous Improvement
- Organisations should consider the extent of applicability of each principle and document how they implement conformance with each principle

Introduction

12. This Chapter outlines the key principles and makes recommendations for the development and operation of an effective Security Incident Management capability.

Principle 1 - Compliance with Legal or Regulatory Requirements

13. All organisations must meet requirements as defined by legislation and their appropriate regulatory bodies. They should therefore determine the level of Security Incident Management capability they require and how compliance with the law or regulatory requirements will be managed. If the organisation has to demonstrate formally its compliance through internal or external reviews then it will need a documented approach to Security Incident Management. In such circumstances the adoption of recognised international standards is recommended; e.g. ISO 27001or ISO/IEC2000:2005

Principle 2 - Business Ownership

14. The business case for developing and maintaining a Security Incident Management capability should be clearly articulated, take account of any regulatory and legal standards, and be endorsed formally at board level. Individual responsibility for developing and owning a Security Incident Management policy should be allocated to a board member.

15. A holistic approach to security management will provide optimum coordination of activity, is likely to be more efficient and deliver the greatest impact from a business perspective. A holistic approach means a coordinated incident response capability across the organisation including personnel, physical and technical security disciplines.

16. Organisations need clear policies regarding their approach to Security Incident Management. This is likely to be a component of the corporate security policy, supplemented by more detailed sub-policies as required. Policy statements should:

a. Create accountability at board level and demonstrate the management commitment to security including reference to security incident response;

b. Establish a Security Incident Management capability and integrate this with other corporate processes such as disaster recovery planning or business continuity management;

c. Clarify responsibilities for applying security controls and for the detection, reporting, investigation, management and resolution of security incidents;

d. Define the service levels required with respect to incident response;

e. Identify how conflicting priorities will be resolved, for example the potential conflict between the restoration of normal business operation and the need to undertake investigation / gather evidence;

f. Promote a culture of security awareness within the organisation, for example by clarifying expected standards in terms of levels of control and behaviours;

g. Promote a learning culture to encourage rapid and full reporting and sharing of incidents across the organisation and its wider IA community

h. Establish clear disciplinary and legal procedures to cover negligent or illegal activity;

i. Include communication strategies to enable effective management of all internal and external stakeholders / relationships;

j. Identify how critical resource areas, such as forensic readiness team, legal or HR, will be secured.

Principle 3 - Planning

17. Organisations should adopt a risk based approach to planning incident management that learns from experience gained within the business, defines the requirements and supporting capability needed with regard for the level of security risk exposure and organisational risk appetite, and integrates incident management with other key corporate processes.

18. Wherever possible planning should be open and collaborative with relevant areas of the organisation to achieve broad acceptance of the approaches and methods used to investigate and manage incidents. Detailed planning should identify the capabilities needed to satisfy the requirement justified in the business case and should identify options for dealing with incidents of varying severity. Integration with higher level business continuity planning will be necessary to be adequately prepared for handling severe incidents

19. Planning should specify the processes, procedures, activities and training necessary to manage incidents effectively and efficiently. It is useful to apply a lifecycle approach to the management of incidents; publicly available standards define a number of lifecycle options which typically include:

a. Prepare – ownership and Advance planning;

b. Monitor, detect and assess incidents to identify severity and initiate appropriate action;

c. Act – contain, eradicate and recover;

d. Learn and apply lessons with respect to the business's internal controls and also with respect to the incident management process itself.

20. These processes / procedures should form the basis of training material for all who are likely to be engaged actively in the incident management process. Procedures for initial reporting should be included in appropriate briefings to all staff and contractors.

21. In today's business environment organisations are increasingly reliant not only on their own, directly-controlled business assets but also on outsourced or shared services. In these circumstances it is even more important that organisations define individual accountabilities in advance and allocate responsibility for incident management activities.

22. Business priorities must be clearly articulated and agreed across the service community (e.g. restoration of business service versus forensic analysis). Understanding who needs to be consulted or informed at any stage is a vital component in the development of an effective communication strategy. Contractual arrangements and SLA metrics should reflect these accountabilities, responsibilities and business priorities and prescribe how changes to these will be managed.

23. Planning will identify the potential range and amount of resources needed and how to acquire, maintain and mobilise them when required. The resources will be varied and will include:-

a. Skills - there are obvious core skills needed for the management of an incident. Advance planning should cater for these core skills but should also identify other skill areas such as Business Continuity, Forensic Analysis (physical or digital), Legal, HR, Communications, Fraud Officer, Internal Audit, Policy, Outside agencies – e.g. emergency services. Where incident response skills do not exist in-house, identify in advance where they can be acquired at short notice eg CESG Certified Cyber Incident Response Service Providers.

b. Information to be accessed and or stored;

c. Access to reporting and support schemes;

d. Accommodation including consideration of any security requirements the incident management team may have;

e. IT, including any test beds that may be required;

f. Office support;

g. Communication options e.g. mobile phones, pagers;

h. Contact lists;

i. Communication strategy to cover engagement with all stakeholders, internal and external, including people who may have been affected by the incident in any way.

24. Planning needs to identify how any of these resources will be accessed in the event of an incident; e.g. if the organisation's IT has been seriously compromised how will the incident team use IT and access / store any information they need? Who are the key contacts and how do you get hold of them inside or outside normal working hours?

25. It is essential that the detailed plans for managing incidents are tested regularly, thoroughly and in realistic circumstances – for example it is wise to undertake some testing at unusual times; it may be easy to get hold of the needed legal, HR or other resources in normal hours but not at 20:00 Hrs on a Friday evening. Testing should also include scenarios that require escalation to Business Continuity Planning and / or Disaster Recovery.

Principle 4 - Information Management

26. Organisations should ensure that the incident management processes capture and store securely all information or records required to provide evidence in legal or disciplinary proceedings, to sustain day to day management and ongoing improvement of the business processes affected and of the incident management process itself. This will inevitably require some level of forensic readiness planning. Procedures covering the use or disclosure of data need to be in accordance with all relevant, legislation, regulation and policy.

27. Effective record capture and management is essential for:-

- Ensuring business operations are effectively restored
- Meeting legal / regulatory requirements
- Improving security controls as required
- Ensuring that the incident management process itself can be managed effectively

Useful guidance on the electronic capture and storage of hard copy can be found at http://www.thecabinetoffice.co.uk/page28.html

28. Data on events, actions taken and decisions made should be captured at the time to improve accuracy and completeness. Information captured (or lost) in the early stages of Security Incidents can make or break the successful restoration of service, the successful prosecution of legal or disciplinary procedures or the capture and application of lessons to be learned. Adoption of a standard format will assist reporting and subsequent analysis of the incident itself or of any trends for example over time or across different types of incident. Automation will improve efficiency and help individuals follow the correct processes. Both International Standards Organisation (ISO) (references [a] and [b]) and European Network and Information Security Agency (ENISA) (reference [c].) provide guidance on what information to collect during an incident life cycle.

29. Clear guidelines on the disclosure or sharing of information with any internal or external recipients need to be established and made available to the incident management team. In certain circumstances information may have to be made available to outside agencies (e.g. law enforcement). More general communications may also be needed, for example to manage reputational damage, to advise customers or users on restoration of service or to advise individuals who may have suffered specific loss, e.g. have had personal data lost or disclosed. In all circumstances organisations must ensure that their communications strategy is compliant with any legal requirements. A clear policy on data retention will also help to secure incident data and reduce the potential risks arising from its accumulation.

30. The true costs of an incident also need to be captured, e.g. those for system downtime, investigations, restoration of full business services, lost business opportunities and damage to corporate reputation or customer confidence. Decisions concerning incident management requirements can then be measured against financial as well as operational risks. At the least an organisation needs to ensure that the increased costs of any additional controls it may consider can be justified by the actual impact and associated costs of the incidents and the likelihood of their recurrence.

Principle 5 - Continuous Improvement

31. Organisations should have a management review process that improves plans for business operations and the incident management process in accordance with experience and technological developments.

32. Effective Security Incident Management will capture sufficient data to identify the root causes of problems. This will enable review of the risk management processes and what, if any, adjustments need to be made to the risk assessments and / or improvements made to the security controls.

33. Incidents are undesirable but inevitable. However, providing they are managed in a planned and systemic manner they provide an opportunity to learn lessons about the management processes affected by the incident and about how well the incident management process itself has worked. A proportionate lessons-learned exercise should be conducted at the conclusion of all incident investigations to identify and address weaknesses and / or build on strengths of the incident management process.

34. Lessons need to be learned at all levels – individual, team, organisation or wider within business sector / Wider IA Community. Organisations need to consider how best to share lessons learned with other like-minded organisations using resources such as the Computer Security and Incident Response Team (CSIRT) or Warning, Advice and Reporting Point (WARP) communities. Promotion of a learning culture to ensure that managers and staff are comfortable to expose the full facts concerning an incident is important. An underlying concept of trust is essential to learning at all levels. If incidents are seen primarily as an opportunity to improve then it is more likely that the full facts will be revealed so improving the chances of understanding what the root

causes are. Swift and complete resolution of the incident will be more likely and sound foundations will be laid for lessons to be learned at all levels.

35. Notwithstanding the need for a learning culture, disciplinary, legal or regulatory processes are required where incidents reveal negligent and or criminal activity. These should be developed and agreed with HR who will be required to play a leading role when such procedures are activated.

Chapter 4 - Implementation

Key Principles

- Maintaining a Security Incident Management capability is potentially expensive and organisations need to consider how best to acquire, structure and maintain the resources needed to deliver the standards of incident management they require proportional to the severity of the incident

Introduction

36. An organisation’s size, purpose, complexity and risk appetite are all factors in deciding how to implement Security Incident Management. The complexities of relationships with other organisations are also important; e.g. is there reliance on shared services or data centres? What critical assets do the organisation’s business operations rely on? Who is responsible for managing incidents affecting those assets? Clarity of responsibility is particularly important where assets or services are shared. Different organisations have different business drivers and it must be clear how any conflict of interest is managed.

Structure

37. Maintaining the authority of the incident response team is crucial. Ideally the team should report directly to the board member responsible for security policy.

38. Understanding the corporate process model and how Security Incident Management interacts within it will identify the major internal interfaces to be maintained. ENISA outline a range of possible models in the context of establishing a Computer Security and Incident Response Team (CSIRT) function. Though this guidance is primarily focussed on the computer security environment many of the principles are more widely applicable.

39. Analysis of the resources required will determine whether they are required full time, part-time or on-call; dedicated to Security Incident Management or sourced from other functions; whether the skill base is maintained internally or outsourced. Regardless of any outsourcing there remains a corporate responsibility to protect its assets; organisations cannot relinquish their responsibilities for implementing effective Security Incident Management.

40. The appropriate structure can only be determined by the organisation itself. A trade-off between cost efficiencies and degrees of control will come into play. Whatever blend of arrangements is used to acquire the resources arrangements should reinforce accountability at board level.

Clarity of Accountabilities and Responsibilities

41. Business environments are becoming more complex and traditional boundaries can become blurred for example through the outsourcing of functions or the use of shared services. In all circumstances an organisation retains the accountability and responsibility for ensuring that it has met its legal and regulatory responsibilities and that it can maintain its business operations into the future. In shared service environments it is critical to establish clear

accountabilities, responsibilities for incident management and to have sufficient processes and procedures that satisfy the essential requirements of all parties and allow for changes to be implemented.

Outsourcing Incident Management Function(s)

42. In a majority of organisations at least some element of incident management is likely to be subcontracted. Contractual arrangements will need to reflect the agreed accountabilities and responsibilities. Performance criteria need to be clearly defined and should avoid potentially dysfunctional behaviours – e.g. compromise corporate policy on the balance between service restoration and investigation or catering for variations of user requirements in a shared services environment.

43. Allowance should be made for changes to the assets supported and to the levels of service required.

44. For complex cyber incidents, CESG and CPNI certify Cyber Incident Response service providers under a joint scheme currently in its pilot phase and due to launch fully in March 2013. Further details are available from www.cesg.gov.uk/servicecatalogue/cir/Pages/Cyber-Incident-Response.aspx

Annex A – HMG Requirements, Activities, Documentation and Points of Contact/Support

Introduction

45. This Annex builds on the fundamental principles outlined in this GPG in the context of HMG Departments and Agencies. It clarifies the formal requirements placed on HMG organisations and identifies specific reporting channels and other points of contact. Annex B to GPG 24 achieves a similar purpose for CNI organisations and may be of interest to some HMG readers. It is up to Departments and Agencies to determine the extent to which this guidance should apply to supporting organisations.

Requirements

46. The requirement for incident management function is embodied in the HMG Security Policy Framework (SPF) (reference [d]). HMG Departments and Agencies **must** establish and operate an effective risk-based Security Incident Management process to comply with Mandatory Requirements (MRs) 7, 9, 44, 48, 69 and 70.

47. HMG IA Standard No 1 & 2 (IS1 & 2), Information Risk Management (reference [e]) mandates the method for technical risk assessment for HMG and provides a good example that other organisations may wish to follow. IS1 & 2 identifies incident management as a component in the minimum mandatory control set. Planning for incident management requires a broader review of business risks in addition to the IS1 & 2 assessment. Departments and agencies will need to draw on other corporate risk management processes to get a more complete understanding of the full risk exposure.

48. HMG IA Standard No 1 & 2 Supplement (IS1 & 2 Supplement) (reference [f]) states that coherent incident management procedures should form part of the corporate IA strategy to enable quick action to minimise potential damage of incidents and provide early identification of wider problems that may need to be addressed. It also mandates and recommends roles that need to be established. Within this context other GPGs provide guidance on specific areas relating to incident management, specifically GPG 13 (reference [g]) Protective Monitoring for HMG ICT Systems and GPG 18 Forensic Readiness (reference [h]),.

Assurance on Security Incident Management capability

49. When developing or maintaining a capability it can be useful to assess current status and progress made against recognised independent standards. The CESG IA Maturity Model (IAMM) and associated assessment framework (reference [i]) was developed to help Departments measure the IA maturity of their processes and to develop an effective improvement programme. Level 1 of the IAMM requires clear policies and processes for reporting, managing and resolving IA incidents. Higher levels require effective learning and sharing of lessons and clarity of related metrics.

50. Although IT focussed, ISO 27001 (reference [a]) provides another framework. ISO have provided a new standard: (reference [b]) - on IT Security Incident Management– ISO 27035:2011 Information Security Incident management –. ISO/IEC2000:2005 (reference [j]) provides another framework within the IT Services Management / IT Infrastructure Library within which incident management plays a structured role.

Accountabilities

51. Accounting Officers are accountable to the Cabinet Office for meeting the mandatory requirements of the SPF and to Ministers for maintaining overall Standards of Internal Control. They have to report formally for protecting business assets and maintaining expected levels of business operation. Departments and Agencies **must** report their compliance status with all SPF MRs in the annual return to the Cabinet Office and the Statement on Internal Control reports to HM Treasury (SPF MR 5 refers). They **must** therefore have documented incident management procedures that can be assessed in order to demonstrate compliance.

52. SPF MR 1 gives further definition of and guidance on the mandatory roles including links to supporting Cabinet Office guidance. IS1 & 2 provides additional guidance on roles required.

Specific Reporting Requirements.

INCIDENT TYPE	POTENTIAL ACTIONS
Any security event including Physical, Personnel or Technical events	1. Report incident to relevant organisational authorities and where appropriate report incident to appropriate regulation authority.
In addition to above	
Technical events eg: Hacking, Denial of Service, Malware (Viruses, trojans etc.) Hardware or Software vulnerabilities	1. Report incident to GovCertUK for information sharing purposes, national security investigations or where other assistance is required. (see appendix B for contact details) (SPF MR 12 refers) 2. If relevant report incident to WARP function or a CPNI Information Exchange where organisation is a member of such a community. 3. Where resolution is beyond the control of local resources, engage a certified Incident Response Service Provider.
Any Criminal Event	1. Report to Police Authorities
Loss of personal data	1. Report within your organisation using appropriate local procedures 2. Report incident to Information Commissioners Office and Cabinet Office (see appendix B for contact details) if the loss is significant taking into consideration the following list which is illustrative and not exhaustive:- Is the loss likely to generate media interest or damage the reputation of the Department or Agency? Is there a risk to personal safety / or of fraud? Does the loss affect more than 25 people (as a guide) or involve vulnerable individuals? Does the loss mean we cannot carry on with our business?
Leaks	1. Follow Cabinet Office Leak Procedures policy document

Central Specialist Support Agencies/ Services and Constituencies Contact Details

Agency	Specific Service	Description of Services offered	Contact Detail	Publications
Government Communications Headquarters (GCHQ)	GovCertUK	GovCertUK is the Computer Emergency Response Team (CERT) for UK Government. We assist public sector organisations in the response to computer security incidents and provide advice to reduce the threat exposure.	**Telephone:** +44 (0)1242 709311 **General Enquiries:** Unclassified: enquiries@govcertuk.gov.uk Restricted: enquiries@govcertuk.gsi.gov.uk **Incidents & Alerts:** Unclassified: incidents@govcertuk.gov.uk Restricted: incidents@govcertuk.gsi.gov.uk	**For more information:** http://www.govcertuk.gov.uk/
	Incident Response Service	Certified Incident Response Service Providers and more information about the service can be found through the CESG web site.	**Add link** **CESG Help Desk phone number**	
Centre for the Protection of National Infrastructure (CPNI)	CPNI Response	CPNI Response assists CNI organisations in managing the response to security incidents and provides holistic advice to reduce the threat to these organisations.	**Telephone:** +44 207 233 8181 **General Enquiries:** enquiries@cpni.gsi.gov.uk **Incidents & Alerts:** response@cpni.gsi.gov.uk	**For more information:** http://www.cpni.gov.uk

Cabinet Office	Information Security and Assurance – breach reporting	Significant breaches of protectively marked data must be reported to the Government Security Secretariat As a general rule, small scale and local breaches of the Data Protection Act involving non-protectively marked information should be managed locally without involving external parties. However, breaches that indicate systemic failure, that could attract national publicity, or that could have a harmful effect on individuals or the organisation's key systems, need to be reported to Ministers, Cabinet Office, Ministry of Justice, the Information Commissioner's Office, and Parliament. Any breaches of personal data that are likely to attract national publicity require notification to Cabinet Office and Ministry of Justice, who will advise on notification to the ICO. Cabinet Office is prepared to advise on the appropriate course of action in case of doubt.	Reporting of classified data breaches: notify.dsi@cabinet-office.x.gsi.gov.uk 020 7276 2990/1403 Reporting of personal data breaches: datareview@cabinet-office.x.gsi.gov.uk 0207 276 3005/3325	Checklist for managing potential loss of data or information – March 2009 Guidance on reporting personal data-related incidents – March 2009
Information Commissioner's Office (ICO)	Regulation of personal data protection.	There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise about what constitutes a large volume of personal data. A reasonable gauge is any collection containing information about 1000 or more individuals, but this figure would reduce as the sensitivity of the data affected increases. Every case must be considered on its own merits. For example it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the data controller is unsure whether to report or not, then the presumption should be to report.	www.ico.gov.uk ICO Helpline: 0303 123 1113	Notification of Data Security Breaches to the Information Commissioner's Office – February 2010

Annex B – CNI Requirements, Activities, Documentation and Points of Contact/Support

Introduction

53. This Annex builds on the fundamental principles of the main GPG in the specific context of CNI organisations. It clarifies the arrangements for providing CPNI support to these organisations, reporting channels and other points of contact.

Requirements

54. Requirement for incident management function

55. CNI organisations are recommended to establish and operate an effective risk-based Security Incident Management process to comply with organisational or regulatory requirements.

56. Assurance on Security Incident Management capability

57. When developing or maintaining such capability it may be useful to assess progress against recognised independent standards. A document that may be of benefit to CNI organisations in this respect is the CESG IA Maturity Model (IAMM) and associated assessment framework developed specifically for UK government to help Departments measure the IA maturity of their processes and to develop an effective improvement programme.

58. Level 1 of the IAMM requires clear policies and processes for reporting, managing and resolving IA incidents. Higher levels require effective learning and sharing of lessons and clarity of related metrics.

59. Although IT focussed, ISO 27001 provides another framework. ISO currently have issued a Standard – ISO 27035:2011 – on Information Security Incident Management

Accountabilities

60. CNI organisations are accountable to their management boards and shareholders, or possibly industry regulators, in meeting INFOSEC or legislative requirements. They may have to report formally on protecting business assets and maintaining expected levels of business operation.

61. There may also be a need to have documented incident management policies and procedures that can be assessed in order to demonstrate compliance.

Specific Reporting Requirements.

INCIDENT TYPE	POTENTIAL ACTIONS
Any security event including Physical, Personnel or Technical events	1. Report incident to relevant organisational security authorities AND where appropriate regulatory authorities.
Technical events eg: Hacking, Denial of Service, Malware (Viruses, trojans etc.) Hardware or Software vulnerabilities	1. Report incident to relevant organisational security authorities and/or Law Enforcement or CPNI for information sharing purposes or national security investigations. (see appendix B for contact details) 2. If relevant report incident to a CPNI Information Exchange or WARP where the organisation is a member of such a community. 3. Where resolution is byond the control of local resources, engage a certified Incidente Response Service Provider.
Any Criminal Event	1. Report to Law Enforcement Authorities
Loss of personal data	1. Report within your organisation using appropriate local procedures 2. Report incident to Information Commissioners Office and Cabinet Office (see CPNI Contact Details for contact details) if the loss is significant taking into consideration the following list which is illustrative and not exhaustive:- Is the loss likely to generate media interest or damage the reputation of the Organisation? Is there a risk to personal safety / or of fraud? Does the loss affect more than 25 people or involve vulnerable individuals? Does the loss mean we cannot carry on with our business?
Leaks	1. Report incident to organisational security authorities, and/or Law Enforcement or CPNI for information sharing purposes

CPNI Contact Details

Agency	Specific Service	Description of Services offered	Contact Detail	Publications
Centre for the Protection of National Infrastructure	CPNI Response	CPNI Response assists CNI organisations in managing the response to security incidents and provides holistic advice to reduce the threat to these organisations.	**Telephone:** +44 207 233 8181 **General Enquiries:** enquiries@cpni.gsi.gov.uk **Incidents & Alerts:** response@cpni.gsi.gov.uk	**For more information:** http://www.cpni.gov.uk
Information Commissioner's Office (ICO)	Regulation of personal data protection.	There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise about what constitutes a large volume of personal data. A reasonable gauge is any collection containing information about 1000 or more individuals, but this figure would reduce as the sensitivity of the data affected increases. Every case must be considered on its own merits. For example it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the data controller is unsure whether to report or not, then the presumption should be to report.	**www.ico.gov.uk** **ICO Helpline: 0303 123 1113**	**Notification of Data Security Breaches to the Information Commissioner's Office – February 2010**

References

[a] ISO/IEC 27001:2005, Information technology - Security techniques – Information security management systems - Requirements.

[b] ISO 27035:2011 - Information Technology – Security Techniques – Information Security Incident Management

[c] ENISA - A Step – By Step Approach On How To Set Up A CSIRT. – http://www.enisa.europa.eu/

[d] HMG Security Policy Framework, Version 8, April 2012. Tiers 1-3 are available at: http://www.cabinetoffice.gov.uk

[e] HMG IA Standard No. 1 & 2, Information Risk Management (UNCLASSIFIED) – latest issue available from the CESG website.

[f] HMG IA Standard No. 1 & 2 Supplement, Technical Risk Assessment and Risk Treatment (UNCLASSIFIED) – latest issue available from the CESG website.

[g] CESG Good Practice Guide No. 13, Protective Monitoring for HMG ICT Systems – latest issue available from the CESG website.

[h] CESG Good Practice Guide No. 18, Forensic Readiness – latest issue available from the CESG website.

[i] HMG IA Maturity Model http://www.cesg.gov.uk/products_services/iacs/iamm/media/iamm-assessment-framework.pdf

[j] ISO/IEC 20000:2005, Information Technology - - Service Management.

[k] Cabinet Office Checklist for managing potential loss of data or information – March 2009

[l] Cabinet Office Guidance on reporting personal data-related incidents – March 2009

Further Reading

[m] GovCertUK alerts and advisories For more information: http://www.govcertuk.gov.uk/

[n] ISO/IEC 27002:2005 Code of Practice for Information Security Management

[o] BS25999 - Business Continuity Management

[p] HMG IA Standard No. 6, Protecting Personal Data and Managing Information Risk – latest issue available from the CESG website.

Additional Sources of Information (for Annex B – also of interest to HMG readers)

[a] The CPNI websites contain a range of documents on a variety of protective security topics, including personnel, physical and information security that may assist organisational security personnel – http://www.cpni.gov.uk

[b] Warning Advice and Reporting Points (WARP) - A WARP is a community based service where members can receive and share up-to-date advice on information security threats, incidents and solutions. Further information can be found at: http://www.warp.gov.uk/Index/indexintroduction.htm

[c] Handbook for Computer Security Incident Response Teams (CSIRTs): http://www.cert.org/archive/pdf/csirt-handbook.pdf

[d] CERT/CC, Carnegie Mellon University: http://www.cert.org/csirts/

This document has been produced by CESG and CPNI. CESG provides advice and assistance on Information Security in support of the UK Government. CPNI is the UK's Centre for the Protection of National Infrastructure. This is general guidance only and is not intended to cover all scenarios or be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Email: enquiries@cesg.gsi.gov.uk